Centro Universitário de Brasília

Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

KLEUBER LÚCIO TORMIM

ANÁLISE DE MATURIDADE DAS POLITICAS DE SEGURANÇA DA INFORMAÇÃO NA GESTÃO PÚBLICA SEGUNDO O COBIT

Brasília

2016

KLEUBER LÚCIO TORMIM

ANÁLISE DE MATURIDADE DAS POLITICAS DE SEGURANÇA DA INFORMAÇÃO NA GESTÃO PÚBLICA SEGUNDO O COBIT

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Lyra

Brasília

2016

KLEUBER LÚCIO TORMIM

ANÁLISE DE MATURIDADE DAS POLITICAS DE SEGURANÇA DA INFORMAÇÃO NA GESTÃO PÚBLICA SEGUNDO O COBIT

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Lyra

Brasília, 07 de março de 2016

Banca Examinadora

_____

Prof. Dr. Maurício Lyra

_____

Prof. Dr. Paulo Rogério Foina

_____

Prof. Dr. Gilson Ciarallo

Dedico este trabalho:

Aos meus pais, meus maiores mestres e orientadores, Halley Tormim e Alba Lúcia.

À minha esposa Fabíola Tormim, meu grande amor, pela compreensão e incentivo constante na minha caminhada acadêmica, profissional e pessoal.

À Coordenação, Professores e todos os funcionários da Pós-graduação em Governança da Tecnologia da Informação do UniCEUB.

Ao Professor Mauricio Lyra, profundo conhecedor em Governança da Segurança da Informação, que me orientou e indicou os caminhos a trilhar.

Aos meus amigos, ouvintes e psicólogos, sempre dispostos a um debate mais crítico no Mendes.

RESUMO

Atualmente, no mundo interconectado, a informação digital é um dos principais ativos de Tecnologia da Informação e necessita ser convenientemente protegida. O uso de boas práticas e frameworks de controle tem ganhado cada vez mais espaço no ambiente corporativo, principalmente na TI. As organizações reconhecem cada vez mais que a segurança deve ser gerenciada como uma questão de risco da empresa, e não apenas como um problema operacional de TI. As organizações têm se empenhado em implantar Políticas de Segurança da Informação e Comunicação, no entanto, a construção dessas POSIC nas organizações, nos últimos anos, vem, em sua grande parte, baseando-se na norma NBR ISO/IEC 27002. Em 2010, um consórcio formado por importantes atores internacionais no cenário da segurança da informação propôs 12 princípios relevantes a serem considerados na construção dessas políticas. O presente trabalho de pesquisa discute esses critérios na análise da política de segurança de 10 organizações da administração pública federal direta. O estudo apresentou um modelo de pesquisa para o levantamento e diagnóstico do nível de maturidade das Políticas de Segurança da Informação e Comunicação nesses órgãos. Uma visão cuidadosa dessas políticas à luz dos critérios mostra que diferente de um cenário homogêneo e linear, como esperado inicialmente, o cenário que se apresenta é heterogêneo e não linear, mostrando grande disparidade entre as empresas analisadas. Por fim este trabalho apresenta as melhores práticas para a construção de uma política de segurança da informação e comunicação adequada, otimizando o uso da governança da segurança da informação e tratando-a como um viabilizador da governança corporativa e uma forma de se ganhar uma vantagem estratégica.

Palavras-chave: Governança da Segurança da Informação. Política de Segurança da Informação e Comunicação. Normas e Padrões de Segurança.

ABSTRACT

Currently, the interconnected world, digital information is one of the main assets of Information Technology and needs to be properly protected. The use of good practices and control frameworks have gained more and more space in the corporate environment, especially in IT. Organizations increasingly recognize that security must be managed as a matter of the company's risk, not just as an operational problem IT. Organizations have been engaged in implementing Security Policy Information and Communication, however, the construction of these policy in organizations in recent years has been, for the most part, based on ISO / IEC 27002 standards in 2010 a consortium of major international actors in the information security scenario proposed 12 principles relevant to consider in the construction of these policies. The senses research paper discusses these criteria in the analysis of 10 security policy organizations direct federal public administration. The study presented a research model for the assessment and diagnosis of the level of maturity of the Information and Communication Security Policies in these organs. A close look at these policies in the light of the criteria shows that different from a smooth and linear scenario as originally hoped, the scenario that presents itself is heterogeneous and non-linear, showing great disparity between the companies analyzed. Finally this paper presents best practices for building a security policy of information and proper communication, optimizing the use of safety information governance and treating it as an enabler of corporate governance and a way to gain a strategic advantage .

Keywords: Security Information Governance. Information Security Policy. Standards and Security.

LISTA DE ABREVIATURAS E SIGLAS

POSIC	Política de Segurança da Informação e Comunicação
SGSI	Sistema de Gestão de Segurança da Informação
TI	Tecnologia da Informação
ISACA	Information Systems Audit and Control Association
ISF	The Information Security Forum
$(ISC)^2$	International Information System Security Certification Consortium

Sumário

INTRODUÇÃO

No mundo atual, globalizado e interativo, temos a capacidade de disponibilizar e absorver uma quantidade considerável de informação, principalmente através dos meios de comunicação e da internet. Nesse cenário, a Gestão de TI ficou mais complexa e a infraestrutura de TI sofre riscos diários de intrusão visando o “roubo” de dados e a disseminação de códigos maliciosos e vírus, o que pode afetar a operação da empresa.

A informação é um dos principais ativos de uma organização e, como qualquer outro ativo importante, é essencial para os negócios e consequentemente necessita ser adequadamente protegida de possíveis ameaças. Conforme o nível de acesso dos vários pontos da empresa à internet, maior é a necessidade de envolver todos os níveis da organização na questão da Gestão de TI e, em especial, na Segurança da Informação.

Com isso, as organizações passaram cada vez mais a ter os seus sistemas de informações e redes de computadores expostos a riscos suscetíveis a prejuízos financeiros.

A fim de mitigar este risco, começou-se a discutir a implementação da Governança de TI na Segurança da Informação das empresas onde seria baseada nos princípios da transparência, independência e prestação de contas como meio para atrair investimentos para as organizações.

Quando levamos em consideração as organizações, a informação toma uma dimensão extremamente importante, pois decisões importantes são tomadas com base na mesma. A segurança da informação é a forma encontrada pelas organizações para proteger os seus dados, através de regras e controles rígidos, estabelecidos, implementados e monitorados constantemente.

É sabido que muitos sistemas de informação não foram projetados para protegerem as informações que geram ou recebem, e essa é uma realidade tanto do setor Público como Privado. A interligação de redes públicas e privadas e o compartilhamento de recursos de informação dificultam o controle e a segurança do acesso, isso porque a computação distribuída acaba se tornando um empecilho à implementação eficaz de um controle de acesso centralizado. O sucesso da implementação de regras e controles rígidos de segurança da informação dependem de diversos fatores tais como: comprometimento de todos os níveis gerenciais; requisitos de segurança claros e

objetivos; política de segurança que reflita o negócio da organização; processo eficaz de gestão dos incidentes da segurança da informação que possam acontecer, dentre outros.

A Governança de TI tem o papel de criar estes controles de forma que a TI trabalhe de uma maneira o mais transparente possível perante os stakeholders.

De acordo com a *IT Governance Institute (2007b)*, a Governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e os objetivos da organização.

A implementação da Governança de TI nas organizações é baseada em guias de melhores práticas, frameworks e normas. Neste trabalho, abordaremos os aspectos de Segurança da Informação, mais precisamente faremos um estudo sobre a Política de Segurança da Informação nas organizações públicas, item imprescindível para a boa Governança de TI destes órgãos.

Sabendo da importância das informações processadas nos órgãos e entidades da Administração Pública Federal, o Presidente da República editou o Decreto nº. 3.505, de 13 de junho de 2000, onde instituiu a Política Nacional de Segurança das Informações, que determina que todos os órgãos e entidades da Administração Pública Federal, direta e indireta tenham uma Política de Segurança da Informação.

A segurança da informação é uma preocupação básica que permeia todas as organizações e compreende aspectos, como confidencialidade, integridade e disponibilidade, visando proteger a informação que é um ativo dos ativos organizacionais mais importantes de uma empresa.

Tendo como princípio a segurança da informação, se faz necessário a construção de políticas voltadas para os temas, como um instrumento viabilizador para que os conceitos, regras e estratégia da organização sejam difundidas, aplicadas e suportadas.

A construção de políticas de segurança da informação ao longo dos anos se baseou basicamente nas normas propostas pela ISO, porém em 2010, um consórcio formado pelo ISACA, ISF e International Information System Security Certification Consortium [(ISC)2], propôs 12 princípios não proprietários, independentes e agrupados em 3 grupos categorizados como Suportar o Negócio, Defender o Negócio e Promover o Comportamento responsável em segurança da informação.

Com base nos princípios propostos pelo consórcio descrito anteriormente, decidiu-se realizar uma pesquisa qualitativa e quantitativa, visando analisar a aderência de políticas da segurança da informação dentro de um nicho de mercado competitivo, sujeito a um número considerável de regulamentações e legislações e com um volume muito alto de dados gerados, classificados, mantidos e protegidos. Devido às características do nicho de mercado, optou-se por buscar políticas dentro de operadoras de telecomunicações que é um segmento no Brasil de ampla concorrência. Conforme demonstrado em pesquisa (LYRA et al., 2016), um olhar atento dessas políticas mostrou-se que diferente de um cenário homogêneo e linear, como esperado inicialmente, o cenário que se apresenta é heterogêneo e não linear, mostrando grande disparidade entre as empresas analisadas.

Para Ferrer (2014), tendo como instrumento direcionador a ISO 27002 e, baseado nos dados levantados dos mesmos órgãos que foram objeto desse estudo, pôde-se verificar que as POSIC dos órgãos da administração pública federal direta estão num nível de maturidade bem diversificado, necessitando de uma melhor orientação a fim de que haja uma maior homogeneidade e maturidade.

Diante dos resultados obtidos nesses estudos, uma dúvida surgiu. Será que nos órgãos da administração pública federal também se apresentará essa mesma disparidade? Com este enfoque, este estudo teve por finalidade apresentar uma análise das melhores práticas para a construção de uma política de segurança da informação utilizando os 12 princípios não proprietários do COBIT no âmbito das organizações da administração pública federal e realizar um estudo comparativo a fim de avaliar a maturidade destes documentos imprescindíveis para estes órgãos.

Este trabalho pretende contribuir com os estudos relacionados às políticas de segurança da informação e verificar se há uma correlação entre a maturidade na adoção da Governança de Segurança da Informação do COBIT e da NBR ISO/IEC 27002 (2005, P. IX) e, busca instrumentalizar as organizações sugerindo uma adoção das boas práticas de Governança de Segurança da Informação dentro das empresas do segmento da administração pública.

Deste objetivo, outros mais específicos se depreendem:

- ✓ Realizar um levantamento da literatura sobre o assunto política de segurança da informação;

- ✓ Analisar as políticas de segurança da informação da administração pública;
- ✓ Apurar a maturidade segundo o COBIT e comparar a maturidade dos órgãos da administração pública em relação aos dois frameworks.

Por ser um tema atual, com grande relevância para as organizações, para compreender estas questões levantadas anteriormente e lançar um olhar sobre as políticas de segurança da informação no contexto destas organizações da administração pública, é que a presente pesquisa foi elaborada.

Sob a ótica acadêmica, a presente pesquisa pretende verificar se existe uma correlação entre esses dois frameworks de Governança de Segurança da Informação.

Apesar da NBR ISO/IEC 27002 (2005, P. IX) indicar que o objetivo da política é "Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes", atualmente não existe um padrão mínimo para as políticas de segurança da informação que cada organização precisa implantar. Este fato evidencia a necessidade de um estudo exploratório desta temática.

Os 12 princípios a serem considerados na construção das políticas de segurança propostos em 2010 pelo consórcio formado por importantes atores internacionais no cenário da segurança da informação complementam a NBR ISO/IEC 27002 (2005, P. IX)? Adotando um framework automaticamente estou em compliance com o outro?

Este estudo se caracteriza por uma avaliação primariamente qualitativa e secundariamente quantitativa, onde será aplicada uma abordagem estruturada em cascata, partindo desde a pesquisa da massa de dados, passando por uma contextualização da mesma, até chegar a uma conclusão extrapolada de inferências baseadas em tabelas e gráficos.

O passo inicial será o levantamento da massa de dados para pesquisa. Nesse passo, buscaremos junto a prestadores de serviços ou funcionários dos órgãos públicos as políticas de segurança.

No passo seguinte, realizaremos uma análise da estrutura e do conteúdo das políticas, de forma, verificar se a forma como foi escrita o texto da política seria mais formal ou mais intuitiva, se sua preocupação primária era ou não atender as normas da

NBR ISO/IEC 27002 (2005, P. IX) e/ou o COBIT e por fim, se os temas foram abordados de forma clara e genérica ou foram abordados de forma específica e pouco genérica.

Subsequentemente, iniciamos uma análise do conteúdo das políticas buscando, menções aos princípios propostos inicialmente e nas normas da NBR ISO/IEC 27002 (2005, P. IX). Cada princípio será analisado individualmente.

Uma vez sendo possível quantificar a aderência de uma política aos princípios propostos, aplicaremos uma escala de maturidade, atribuindo, de acordo com a quantidade de itens aderentes, um nível de maturidade para cada empresa e uma análise comparativa será realizada com os resultados obtidos utilizando a NBR ISO/IEC 27002 (2005, P. IX).

Para alcançar esses objetivos, realizamos pesquisa bibliográfica em artigos científicos, monografias e dissertações de mestrado nos repositórios da Universidade de Brasília - UnB e do Centro Universitário de Brasília – UniCEUB, assim como também fizemos uma pesquisa em livros técnicos especializados que tratam do assunto de Segurança da Informação. Mapeamos as melhores práticas para criação de uma POSIC para as organizações por meio das normas da família ISO/IEC 27000. Realizamos uma pesquisa na web da POSIC de dez órgãos da administração pública federal direta, onde escolhemos órgãos de diferentes áreas de atuação (estratégico, fundamental e especial), com intuito de realizarmos uma análise comparativa destas POSIC com as melhores práticas levantadas. E, por fim, realizamos uma análise crítica e comparativa de forma a apresentarmos uma matriz com o nível de maturidade das POSIC das organizações analisadas, assim como uma análise destas POSIC conforme suas áreas de atuação.

O presente trabalho foi estruturado em três capítulos. Inicia-se o trabalho com a introdução, onde faz referência ao tema, definição, objetivos gerais e específicos, a metodologia utilizada e por fim uma breve explicação da estrutura do trabalho.

No primeiro capítulo, inicia-se com conceitos relacionados à segurança da informação, tais como os princípios, governança da segurança, modelos, normas e padrões relacionados ao tema.

No capítulo seguinte, abordam-se aspectos de uma Política de Segurança da Informação e Comunicação, apresentando informações sobre a estruturação de uma

POSCI, assim como uma análise crítica deste documento e os requisitos necessários que contemplam uma política adequada segundo as melhores práticas.

No terceiro capítulo, analisam-se as POSIC de dez órgãos da administração pública federal, onde se apresenta uma matriz com o grau de maturidade destas POSIC e gráficos de tendências.

No final, apresenta-se a conclusão do trabalho.

1 SEGURANÇA DA INFORMAÇÃO

1.1 Definição da Segurança da Informação

A NBR ISO/IEC 27002 (2005, P. IX) define a informação com sendo “um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida”. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

A informação pode surgir de diversas formas, seja pelo meio físico como impressões de documentos ou escrita em papel, ou digital como trocas de e-mails ou armazenada eletronicamente. Seja qual for o meio que a informação é compartilhada ou armazenada, ela precisa ser adequadamente protegida.

Para Beal (2005), segurança da informação pode ser entendida como o processo de proteger informações das ameaças para garantir a sua integridade, disponibilidade e confidencialidade. Porém, segurança da informação não pode ser encarada como “guardar em um cofre todas as informações disponíveis”, mas sim elaborar uma boa política de proteção evitando riscos e vulnerabilidade.

> Segundo a NBR ISO/IEC 27002 (2005, P. IX), Segurança da Informação é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Fontes (2006) define a Segurança da Informação como um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada.

1.2 Princípios da Segurança da Informação

Segurança é a base para dar às empresas a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócio. É evidente que os negócios estão cada vez mais dependentes das tecnologias e estas precisam estar de tal forma a proporcionar confidencialidade, integridade e disponibilidade – que conforme a NBR

ISO/IEC 27002 (2005, P. IX), são os princípios básicos para garantir a segurança da informação – das informações.

> Quando se pensa em segurança da informação, a primeira ideia que nos vem à mente é a proteção das informações, não importando onde estas informações estejam armazenadas. Um computador ou sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como o esperado. Porém a segurança não é apenas isto.
>
> A expectativa de todo o usuário é que as informações armazenadas hoje em seu computador, lá permaneçam, mesmo depois de algumas semanas, sem que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo. (DIAS, 2000 apud SPANCESKI, 2004).

Os cinco pilares da Segurança da Informação, conhecidos como C.I.D.A.L - Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade - representam os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

1.2.1 Confidencialidade

É a propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo dono da informação.

Para Spanceski (2004), a informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital. O objetivo da confidencialidade é proteger a informação privada (cidadãos, indústrias, governo, militar) contra o acesso por alguém não autorizado interna ou externamente.

O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.

1.2.2 Integridade

É a propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição). A

informação deve ser retornada em sua forma original no momento em que foi armazenada.

O item integridade não pode ser confundido com confiabilidade do conteúdo (seu significado) da informação. Uma informação pode ser imprecisa, mas deve permanecer integra (não sofrer alterações por pessoas não autorizadas).

1.2.3 Disponibilidade

É a propriedade que garante o acesso às informações sempre que for necessário por pessoas autorizadas.

Para Spanceski (2004), a disponibilidade consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao utilizador o acesso aos dados sempre que deles precisar.

Segundo Dias (2000 apud SIEWERT, s/d) a disponibilidade protege os serviços de informática de tal forma que não sejam degradados ou fiquem indisponíveis sem a devida autorização. Para um utilizador autorizado, um sistema não disponível quando se necessita dele, pode ser tão ruim quanto um sistema inexistente ou destruído.

As medidas relacionadas a esse objetivo, podem ser a duplicação de equipamentos ou backup, disponibilidade pode ser definida como a garantia de que os serviços prestados por um sistema são acessíveis, sob demanda, aos utilizadores autorizados. (DIAS, 2000 apud SIEWERT, 2004).

1.2.4 Autenticidade

É a propriedade que garante que em um processo de comunicação, os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

Autenticidade é a certeza de que um objeto (em análise) provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo. Na telecomunicação, uma mensagem será autêntica se for, de fato, recebida na íntegra, diretamente do emissor.

A verificação de autenticidade é necessária após todo processo de identificação seja de um usuário para um sistema ou de um sistema para outro sistema. A autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos. (SPANCESKI, 2004)

1.2.5 Legalidade

É a propriedade que garante que as informações foram produzidas respeitando a legislação vigente.

Legalidade é a característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas, normas internas de uma corporação ou a legislação política institucional, nacional ou internacional, ou seja, garante a legalidade jurídica da informação.

A figura 1 abaixo nos apresenta como os princípios da segurança da informação se relacionam.

Figura 1 - Princípios da Segurança da Informação

Fonte: Elaborado pelo autor (2015)

1.3 Ameaças e vulnerabilidades à Segurança da Informação

As ameaças aproveitam das falhas de segurança da organização, que é considerado como ponto fraco, provocando possíveis danos, perdas e prejuízos aos negócios da empresa. O conceito de ameaça é definido por possíveis danos aos ativos, intencionais ou não.

Ameaças são subdivididas em: desastres naturais, tais como, fogo, enchentes e terremotos, humanas, que são subdividida em intencional, onde ocorre diretamente por hackers e funcionários descontentes e não intencional, onde funcionários com pouco conhecimento sobre a tecnologia aplicada e ambientais, que engloba toda parte tecnológica como software, hardware, falhas de sistema operacional e falha elétrica.

Para Sêmola (2003), ameaças são os meios pelos quais a confidencialidade, integridade e disponibilidade da informação podem ser comprometidas.

Na perspectiva do mesmo autor Sêmola (2003), vulnerabilidade são as circunstâncias que aumentam a possibilidade de uma ameaça ser concretizada, elevando

sua frequência e seu impacto. Na análise do risco, vulnerabilidade é a falta de segurança para determinado ativo ou grupo de ativos.

Corrigir pontos vulneráveis ou pontos fracos que circulam em um setor que trabalha com a informação, não acabará, mas reduzirá em muito os riscos em que ela estará envolvida. Logo estará evitando como também prevenindo a concretização de possíveis ameaças.

No entanto, não poderia deixar de citar o autor Wadlow (2000), onde nos mostra que as vulnerabilidades são os pontos fracos existentes nos ativos, que quando explorados por ameaças, afetam a confiabilidade, a disponibilidade e a integridade das informações de uma pessoa ou organização.

Identificar e eliminar os pontos fracos de um ambiente de tecnologia da informação é um dos primeiros passos para garantir uma melhora na segurança da informação. Quando identificado às vulnerabilidades, os riscos ficarão melhores dimensionados nos locais que estão expostos, facilitando assim, a definição de uma medida de segurança para fazer a correção.

Políticas inadequadas podem levar a problemas de segurança, da mesma forma usuários podem potencialmente fazer o mau uso de seus direitos e violar a segurança dos ativos da empresa (SENGUPTA; MAZUMDAR; BAGCHI, 2009)

1.4 Governança de Segurança da Informação

Para entendermos melhor o significado da palavra Governança, podemos recorrer ao dicionário Aurélio, encontraremos “governar, que é por sua vez significa administrar, reger, dirigir, regular o andamento de algo, conduzir, monitorar”.

No site do Instituto Brasileiro de Governança Corporativa (IBGC) encontramos a seguinte definição para Governança.

> É o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo as práticas e os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e aperfeiçoar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade. (IBGC, 2014)

Analisando a definição de Governança pelo IBGC, podemos concluir que a Governança é responsável pela implantação de boas práticas e por promover a transparência, a prestação de contas, equidade e a responsabilidade corporativa nas organizações.

Quando falamos em Governança, vem a nossa cabeça a Governança Corporativa ou Governança de Tecnologia da Informação, mas como vimos na definição da palavra anteriormente, o termo está ligado ao controle, ao regulamento ou monitoramento.

De acordo com Lyra (2015), a Governança é um tema muito presente na sociedade moderna, pois procura apresentar o sistema pelo qual as organizações são dirigidas e monitoradas, melhorando a transparência e a responsabilização das decisões nas corporações. A governança é um tema multifacetado e por isso a Governança da Segurança da Informação exerce seu papel trazendo o foco da discussão para a Segurança da Informação.

Abordaremos nesse trabalho a Governança de Segurança da Informação.

No ano de 2013 foi publicada a Norma ABNT NBR ISO/IEC 27014:2013 - Tecnologia da Informação - Técnicas de Segurança – Governança de Segurança da Informação, que descreve as ações para a implantação da Governança de Segurança da Informação. Os objetivos da Governança de Segurança da Informação, segundo a norma são:

- ✓ Alinhe aos objetivos e a estratégias da Segurança da Informação com os objetivos e estratégias do negócio da organização;
- ✓ Agregar valor para a alta direção e para as partes interessadas;
- ✓ Garantir que os riscos da informação estão sendo adequadamente endereçados para a pessoa responsável;

Uma vez implantada, os resultados eficientes e eficazes da Governança de Segurança da Informação são:

- ✓ Visibilidade da alta direção sobre a situação da Segurança da Informação;
- ✓ Uma abordagem ágil para a tomada de decisões sobre os riscos da informação;
- ✓ Investimentos eficientes e eficazes em Segurança da Informação;
- ✓ Conformidade com requisitos externos: legais, regulamentares ou contratuais;

A Norma ABNT NBR ISO/IEC 27014:2013 também define os princípios para a Governança de Segurança da Informação. São esses princípios que informam como a Segurança da Informação será utilizada no negócio.

- ✓ **Principio 1** - Estabelecer a Segurança da Informação em toda a organização;
- ✓ **Principio 2** - Adotar uma abordagem baseada em riscos;
- ✓ **Principio 3** - Estabelecer a direção de decisões de investimento;
- ✓ **Principio 4** - Assegurar conformidade com os requisitos internos e externos;
- ✓ **Principio 5** - Promover um ambiente positivo de segurança;
- ✓ **Principio 6** - Analisar e criticar o desempenho em relação aos resultados de negócio;

No entanto, o framework mais recomendado para implantação da Governança de Segurança da Informação é o COBIT, a versão 5 foi lançada em 2012 e é considerado, por muitos, como a base para a Governança de Tecnologia da Informação, pois ajuda as organizações a criarem valor para TI, mantendo o equilíbrio entre os investimentos em recursos e os riscos organizacionais. Consideram os negócios, as áreas funcionais de TI da empresa e as partes interessadas, tanto internas como externas. Empresas de todos os tamanhos sejam elas comerciais, sem fins lucrativos ou do setor público.

O COBIT 5 é baseado em cinco princípios fundamentais para a governança e gestão de organizações de TI:

1. Reunir as necessidades dos stakeholders;
2. Cobrir a empresa fim-a-fim;
3. Aplicar um framework único e integrado;
4. Aplicar uma abordagem holística;
5. Separar a governança da gestão;

O COBIT 5 descreve ainda sete categorias de facilitadores:

1. Princípios, políticas e quadros são métodos para traduzir o comportamento desejado em orientações práticas para o dia-a-dia de gestão.
2. Os processos descrevem um conjunto organizado de práticas e atividades para atingir certos objetivos e produzir um conjunto de saídas para atingir as metas de TI.
3. As estruturas organizacionais são as principais entidades de tomada de decisão em uma empresa.

4. A cultura, a ética e o comportamento dos indivíduos e da empresa são muitas vezes subestimadas como fator de sucesso em atividades de governança e gestão.
5. A informação é necessária para manter a organização funcionando e bem governada, mas no nível operacional, a informação é muitas vezes a chave do produto da própria empresa.
6. Os serviços, a infraestrutura e as aplicações fornecem às empresas os recursos necessários para o processamento de informação.
7. As pessoas, habilidades e competências são necessárias para a conclusão bem-sucedida de todas as atividades, e para tomar decisões corretas e ações corretivas.

Por ter sido concebido com base em diversas normas e pelas boas práticas do mercado de Tecnologia da Informação, o COBIT 5 possui uma flexibilidade de atuação com outras normas e metodologias que outros padrões não possuem. Além disso, suas comunicações com os objetivos estratégicos do negócio são muito claras, o que permite realizar a integração da Segurança da Informação ao negócio de forma simples (MANOEL, 2014 pg 30).

1.5 Modelos para Segurança da Informação

A origem de praticamente todas as normas internacionais relativas à segurança é o Governo Britânico".

A British Standard (BS) 7799, que deu origem à ISO 17799 e que foi substituída em 2005 pela ISO/IEC 27002, nasceu no *Commercial Computer Security Center* (CCSC) do *Department of Trade and Industry*. O CCSC foi criado considerando duas frentes de atuação: a primeira era apoiar fornecedores de produtos de segurança de TI a partir de conjunto de critérios de avaliação e um esquema de certificação, e a segunda era auxiliar os usuários de TI através de um "Código de Prática do Usuário". Este código foi publicado em 1989.

O código foi aperfeiçoado posteriormente pela comunidade britânica de TI, o que resultou no "Código de prática para a gestão da segurança da informação". Esse código deu origem em 1995 à BS 7799:1995, parte 1.

Em abril de 1999, foi publicada a primeira revisão da BS 7799 Parte 1 (BS7799:1999). Em outubro de 1999 esta norma foi proposta como ISO, dando origem, em dezembro de 2000, à ISO/IEC 17799:2000.

A parte 1 da BS 7799 era somente um código de prática e não permitia a certificação de um sistema de gestão de segurança da informação, conforme um esquema de certificação reconhecido mútuo em âmbito internacional. Para suprir essa necessidade, em setembro de 2002 foi lançada a parte 2 da BS 7799 (BS7799-2:2002). Essa norma está em harmonia com a ISO 9000 e a ISO 14000.

Da mesma forma como ocorreu com a 17799, a BS 7799-2:2002 transformou-se na ISO/IEC 27001:2005, publicada em 15 de outubro de 2005.

A série 27000 agrupa a família de segurança da informação relacionado aos padrões ISO, conforme abaixo:

1. ISO/IEC 27000:2012 - Vocabulário de Gestão da Segurança da Informação.
2. ISO/IEC 27001:2013 - Esta norma foi publicada em outubro de 2005 e substituiu a norma BS 7799-2 para certificação de sistema de gestão de segurança da informação.
3. ISO/IEC 27002:2013 - Esta norma trata do Código de prática para controles da segurança da informação e substituiu a ISO/IEC 27002:2005.
4. ISO/IEC 27003:2010 - Esta norma aborda as diretrizes para Implementação de Sistemas de Gestão de Segurança da Informação, contendo recomendações para a definição e implementação de um sistema de gestão de segurança da informação.
5. ISO/IEC 27004:2009 - Esta norma disciplina sobre as métricas e relatórios de um sistema de gestão de segurança da informação.
6. ISO/IEC 27005:2011 - Esta norma será constituída por indicações para implementação, monitoramento e melhoria contínua do sistema de controles. O seu conteúdo deverá ser idêntico ao da norma BS 7799-3:2005 – “Information Security Management Systems - Guidelines for Information Security Risk Management”, a publicar em finais de 2005. A publicação da norma ISO 27005 ocorreu em 2008.
7. ISO/IEC 27006:2011 - Esta norma especifica requisitos e fornece orientações para os organismos que prestem serviços de auditoria e certificação de um sistema de gestão da segurança da informação.
8. ISO/IEC/IEC 27007:2011 - Esta Norma fornece diretrizes sobre como gerenciar um programa de auditoria de sistemas de gestão da segurança da informação (SGSI) e sobre como executar as auditorias e a competência de auditores de SGSI.

A ISO/IEC 27001 foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da

informação (SGSI), já a ISO/27002 foi projetada para organizações que usam a norma como uma referência para selecionar controles dentro do processo de implementação do sistema de gestão de segurança da informação ou como um guia para implementar controles aceitos de segurança da informação. Vide ISO (2013).

A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, exigências de segurança, os processos empregados e o tamanho e estrutura da organização.

1.5.1 Estrutura do Modelo ISO/IEC 27001

A versão 2013 desta norma aplica a estrutura de alto nível, os títulos de subseções, textos, termos comuns e definições básicas, apresentadas no anexo SL da ISO/IEC *Directives, Part 1, Consolidaded ISO Supplement*, mantendo dessa forma compatibilidade com outras normas de gestão.

Essa abordagem é útil para as organizações que escolhem operar um único sistema de gestão que atenda aos requisitos de duas ou mais normas de sistemas de gestão.

Seguindo os conceitos de sistema de gestão a norma preconiza:

- ✓ Que o contexto do sistema de gestão de segurança da informação seja compreendido, inclusive a determinação do seu escopo.
- ✓ A liderança necessária para a implementação do SGSI, considerando o comprometimento da administração, a existência de uma política e a autoridade, responsabilidade e papéis organizacionais.
- ✓ O planejamento do SGSI, considerando ações para contemplar riscos e oportunidades, a determinação dos objetivos do sistema.
- ✓ O apoio necessário para o sistema em termos de recursos, competências, conscientização, comunicação e a informação documentada.
- ✓ A operação do sistema, considerando o planejamento organizacional, a avaliação dos riscos de segurança da informação, o tratamento dos riscos.
- ✓ A avaliação do desempenho do sistema, contemplando monitoramento, medição e análise e avaliação, a auditoria interna e a análise crítica pela direção.

- ✓ Por fim, a melhoria do sistema, contemplando o tratamento de não conformidades e ações corretivas, e a melhoria contínua.

1.5.2 Estrutura do Modelo ISO/IEC 27002

Independentemente dos aspectos de certificação, este modelo se aplica a qualquer organização cujos negócios dependam fortemente de informação de TI.

Segundo Fernandes e Abreu (2014), a utilização de um modelo nesses moldes para as empresas de serviços de TI é praticamente obrigatória, por proporcionar maior garantia de proteção de ativos de informação do cliente, significando garantia de continuidade dos serviços para o cliente.

A amplitude da segurança da informação é bem maior do que somente TI, abrangendo também, e fortemente, as áreas finem a classificação da informação, se de negócio, pois são elas que definem privilégios de acesso e de definem a classificação da informação, se é confidencial, de uso interno ou público.

Entretanto, a implantação de SGSI, por ser amplo e abranger também as unidades de negócio, necessita de um forte patrocínio dentro da organização, assim como de um programa contínuo de conscientização e de um pesado envolvimento da área de recursos humanos e das áreas que faze contratação e uso de terceiros.

Os benefícios de se utilizar o modelo estão na prevenção de perdas financeiras que a organização pode ter, no caso da ocorrência de incidentes de segurança da informação. A organização também pode abalar a sua imagem ou sofrer ações na justiça pelas perdas que seus sistemas possam causar aos clientes.

De acordo com a norma NBR ISO/IEC 27002:2013, temos 14 (quatorze) seções de controle de segurança da informação com os seus respectivos objetivos, os quais são dispostos abaixo, onde também há as considerações de alguns autores referenciados sobre estes controles.

1.5.2.1 Política de Segurança da Informação

Segundo a NBR ISO/IEC 27002:2013, o objetivo primordial de uma POSIC é prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

> Para Castro (2002), a Política de Segurança da Informação é basicamente um manual de procedimentos que descreve como os recursos de que manipulam as informações da empresa devem ser protegidos e utilizados, e é o pilar da eficácia da Segurança da Informação, estabelecendo investimentos em recursos humanos e tecnológicos.

A elaboração da Política de Segurança deve considerar os processos, os negócios, toda e qualquer legislação que os envolva, os aspectos humanos, culturais e tecnológicos da organização. Ela servirá de base para a criação de normas e procedimentos que especificaram as ações no nível micro do ambiente organizacional, além de ser facilitadora e simplificadora do gerenciamento dos demais recursos da organização (NAKAMURA; GEUS, 2003).

1.5.2.2 Organização da Segurança da Informação

Segundo a NBR ISO/IEC 27002:2013, a organização da segurança da informação deve estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.

1.5.2.3 Segurança em Recursos Humanos

A NBR ISO/IEC 27002:2013 disciplina que a organização deve ter como objetivo reduzir os riscos de erro humano, roubo, fraude assim como o uso indevido das instalações. Para isto, deve-se observar que as responsabilidades de segurança sejam atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a vigência de todo o contrato de trabalho do funcionário.

De acordo com Rezende e Abreu (2000), as organizações devem procurar dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório. Dessa forma, seria importante destacar que o elo mais fraco de um processo

de segurança é a pessoa (ou grupos de pessoas), que por sua vez, é a responsável por garantir a fidelidade da informação.

Para mitigar riscos quanto aos recursos humanos a serem contratados numa organização, a NBR ISO/IEC 27002:2013 disciplina que antes da contratação deste profissional, seja verificado o histórico do candidato ao emprego de acordo com a ética, regulamentações e leis relevantes. Ainda, disciplina que durante a contratação, a direção deve solicitar a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização. Para que este requisito seja essencialmente cumprido por todos, é recomendado que a direção demonstre seu total apoio às políticas, procedimentos e controles, e aja como tal, de forma exemplar.

> Segundo Spanceski (2004) dentre os controles considerados como melhores práticas para a segurança da informação temos: definição das responsabilidades na segurança da informação e educação e treinamento em segurança da informação.

Da mesma forma, a NBR ISO/IEC 27002:2013 ratifica que a conscientização, educação e treinamento em segurança da informação deve ser prevista para todos os funcionários da organização e, quando pertinente, para as partes externas intervenientes.

Quanto ao encerramento do contrato do funcionário, a NBR ISO/IEC 27002:2013 disciplina que as responsabilidades e obrigações pela segurança da informação devem estar previstas mesmo após o encerramento do contrato.

1.5.2.4 Gestão de Ativos

A NBR ISO/IEC 27002:2013 disciplina que os ativos da organização devem ser devidamente identificados por meio de um inventário de ativos estruturado. Além do que, sempre deve haver um proprietário para este inventário de ativos.

Quanto a classificação da informação, esta norma, disciplina que tem como objetivo assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização. Esta classificação deve ser incluída nos processos da organização e ser consciente e coerente em toda a organização.

A classificação da informação é importante para que as organizações possam determinar o nível de proteção das informações, de modo que a segurança das

informações nas organizações possa ser assegurada. (DIAS, 2000 apud SPANCESKI, 2004).

De acordo com Sêmola (2003, p. 106, grifo nosso), os critérios normatizados para admissão e demissão de funcionários, criação e manutenção de senhas, descarte de informação em mídia magnética ou em papel, desenvolvimento e manutenção de sistemas, uso da internet, acesso remoto, uso de notebooks, contratação de serviços terceirizados e classificação das informações, são alguns exemplos de normas de uma típica Política de Segurança da Informação.

Para que a gestão de ativos seja efetiva, a NBR ISO/IEC 27002:2013 descreve que as mídias devem ser adequadamente tratadas a fim de prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias. Esta norma, também destaca que o descarte de mídias deve ser realizado de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.

1.5.2.5 Controle de Acesso

Segundo a NBR ISO/IEC 27002:2013, a organização deve ter como objetivo imitar o acesso à informação e aos recursos de processamento da informação. Para que este controle seja atendido plenamente pela organização, esta deve adotar uma política de controle de acesso, gerenciamento de acesso do usuário, definir as responsabilidades dos usuários e um controle de acesso aos sistemas e aplicações.

> Segundo Monteiro e Boavida (2000), a capacidade de impedir o acesso não autorizado a um recurso é, genericamente, designada por controle de acesso. Por vezes são incluídas na categoria de controlo de acesso as funções que limitam a quantidade de recursos a utilizar, o que é correto de um ponto de vista de segurança.

O processo mais adequado quando se pensa em manter o controle efetivo sobre os acessos aos sistemas é propor processos com intervalos periódicos para a revisão das contas de usuários e seus respectivos privilégios no sistema da organização (FERREIRA; ARAUJO, 2006, p.71).

1.5.2.6 Criptografia

Conforme descrito na NBR ISO/IEC 27002:2013, os Controles Criptográficos devem assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

A criptografia é utilizada visando proteger as informações que são consideradas de risco e para as quais outros controles não fornecem proteção adequada. O controle criptográfico deve levar em conta se é apropriado e qual tipo deve ser aplicado (FERREIRA; ARAUJO, 2006, p.78).

Para Tadano (2002), a criptografia é a arte ou ciência de escrever em cifra ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem ilegível, chamado de texto cifrado, de forma a permitir que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza (…).

Na perspectiva de Laureano (2005), a criptografia representa um conjunto de técnicas que são usadas para manter a informação segura. Estas técnicas consistem na utilização de chaves e algoritmos de criptografia. Tendo conhecimento da chave e do algoritmo usado é possível desembaralhar a mensagem recebida.

1.5.2.7 Segurança Física e Ambiental

A Política de Segurança Física precisa considerar o planejamento das instalações, gerenciamento e procedimentos de recuperação de desastres. O objetivo é garantir a segurança da infraestrutura da empresa, deve contemplar a localização dos equipamentos, a construção e o controle de acesso às instalações e planos de contingência (MARTINS, 2003).

> Segundo Fontes (2006), a segurança não envolve somente o ambiente de tecnologia. Existe outra preocupação, que normalmente é tratada com uma certa indiferença, que é a segurança física. As ameaças internas podem ser consideradas como o risco número um à segurança da informação. Um bom programa de segurança física é passo inicial para a defesa da corporação no sentido de proteger as suas informações contra acessos indevidos.

Consoante com a NBR ISO/IEC 27002:2013, a organização deve prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização. Quanto aos equipamentos, convém que estes sejam protegidos e colocados em locais seguros de forma a reduzir os riscos de

ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

Qualquer acesso às dependências da organização, desde as áreas de trabalho até àquelas consideradas severas (onde ocorre o processamento das informações críticas e confidenciais) deve ser controlado sempre fazendo necessária sua formalização (FERREIRA; ARAÚJO, 2008).

1.5.2.8 Segurança das Operações

Segundo a NBR ISO/IEC 27002:2013, a organização deve garantir a operação segura e correta dos recursos de processamento da informação. Os procedimentos de operação devem ser documentados e disponibilizados para todos os usuários que necessitem deles.

Esta norma ainda informa que convém que os procedimentos de operação especifiquem:

a) A instalação e configuração de sistemas;
b) Processamento e tratamento da informação, tanto automática como manual;
c) Cópias de segurança;
d) Requisitos de agendamento, incluindo interdependências com outros sistemas, a primeira hora para início da tarefa e a última hora para o término da tarefa;
e) Instruções para tratamento de erros ou outras condições excepcionais, que possam ocorrer durante a execução de uma tarefa, incluindo restrições de uso dos utilitários do sistema;
f) Contatos para suporte e escalação, incluindo contatos de suporte externos, para o caso de eventos operacionais inesperados ou dificuldades técnicas;
g) Instruções quanto ao manuseio de mídias e saídas especiais, como o uso de formulários especiais ou o gerenciamento de dados confidenciais, incluindo procedimentos para o descarte seguro de resultados provenientes de rotinas com falhas;
h) Procedimento para o reinício e recuperação em caso de falha do sistema;
i) Gerenciamento de trilhas de auditoria e informações de registros (logs) de sistemas;
j) Procedimentos de monitoramento.

Ferreira e Araújo (2006, p.86) citam que o backup é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de algum ataque ou dano as

informações da empresa. Por isso, cabe a instituição levar em consideração a importância da informação que tem, classificando-a adequadamente, levando em conta sua periodicidade de atualização e sua volatilidade para saber o que deve realmente proteger.

A NBR ISO/IEC 27002:2013 também disciplina que a auditoria de sistemas de informação deve seguir atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais de forma que sejam cuidadosamente planejados e acordados para minimizar interrupção de processos do negócio.

1.5.2.9 Segurança das Comunicações

A NBR ISO/IEC 27002:2013 disciplina que a organização para atender este controle de segurança deve observar o gerenciamento da segurança em redes, segurança dos serviços de rede, segregação de redes, transferência de informação, políticas e procedimentos para transferência de informações, acordos para transferência de informações, proteção adequada às mensagens eletrônicas e acordos de confidencialidade e não divulgação.

A segurança lógica envolve aspectos de prevenção contra interceptação e modificação de informações, sigilo no tráfego dos dados na rede, alterações de softwares, invasões em sistema, acessos não a autorizados a informação e demais aspectos relacionados ao aceso e manipulação dos dados da empresa. (SOUSA, 2006).

1.5.2.10 Aquisição, Desenvolvimento e Manutenção de Sistemas

Segundo a NBR ISO/IEC 27002:2013, a organização para atender este controle de segurança deve observar os requisitos de segurança de sistemas de informação, de segurança em processos de desenvolvimento e de suporte e, por fim, assegurar a proteção dos dados usados para teste.

1.5.2.11 Relacionamento com Fornecedores

A NBR ISO/IEC 27002:2013 disciplina a organização para atender os seguintes controle de segurança:

a) A segurança da informação na cadeia de fornecedores;
b) A política de segurança da informação no relacionamento com os fornecedores;
c) A segurança da informação nos acordos com fornecedores;
d) A cadeia de fornecedores na tecnologia da informação e comunicação;
e) O gerenciamento da entrega do serviço do fornecedor;
f) O monitoramento e análise crítica de serviços com fornecedores; e
g) O gerenciamento de mudanças para serviços com fornecedores.

1.5.2.12 Gestão de Incidente de Segurança da Informação

De acordo com a NBR ISO/IEC 27002:2013 para assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação, deve-se atentar com:

a) Responsabilidades e procedimentos;
b) Notificação de eventos de segurança da informação – os eventos de segurança da informação devem ser relatados por meio dos canais de gestão, o mais rapidamente possível;
c) Notificação das fragilidades de segurança da informação;
d) Avaliação e decisão dos eventos de segurança da informação;
e) Resposta aos incidentes de segurança da informação;
f) Aprendizado com os incidentes de segurança da informação; e
g) Coleta de evidências.

1.5.2.13 Aspectos de Segurança da Informação da Gestão da Continuidade de Negócios

De acordo com a NBR ISO/IEC 27002:2013, é prudente que a continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização. A organização deve determinar quais são seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, como por exemplo, durante uma crise ou desastre.

A organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa.

Por fim, é prudente que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.

De acordo com Sêmola (2003), a gestão de continuidade do negócio tem como objetivo permitir a continuidade de processos e informações essenciais à sobrevivência da organização, no menor intervalo de tempo possível, com vistas a evitar/minimizar os impactos de incidentes.

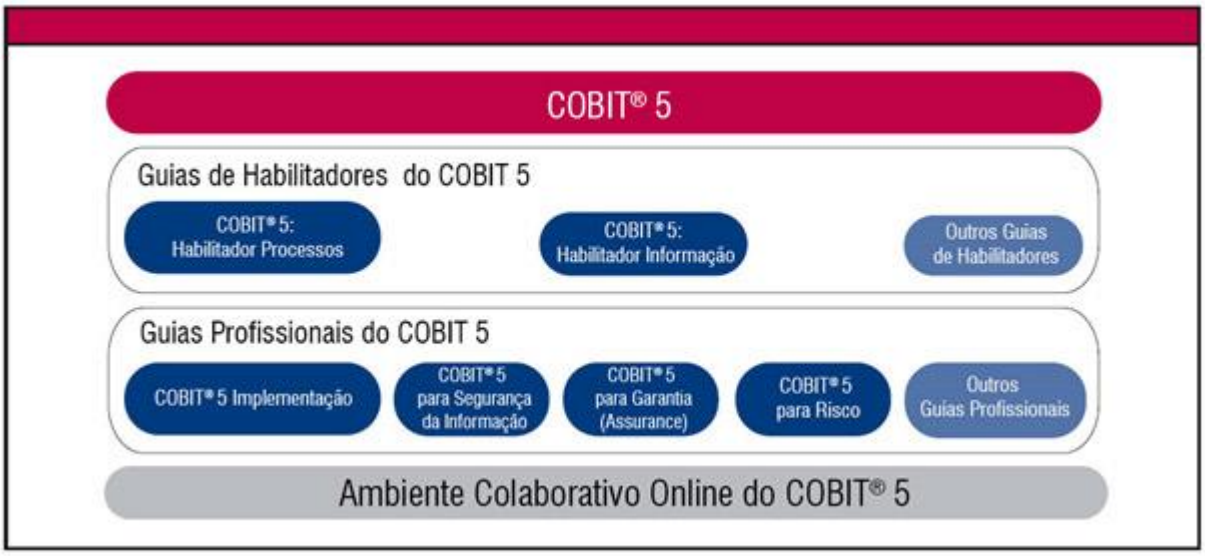
1.5.2.14 Conformidade

Conforme a NBR ISO/IEC 27002:2013, a organização para atender este controle de segurança deve observar: conformidade com requisitos legais e contratuais; identificação da legislação aplicável e de requisitos contratuais; direitos de propriedade intelectual; proteção de registros; proteção e privacidade de informações de identificação pessoal; regulamentação de controles de criptografia; análise crítica da segurança da informação; análise crítica independente da segurança da informação; conformidade com as políticas e procedimentos de segurança da informação; e análise crítica da conformidade técnica.

1.5.3 Estrutura do Modelo COBIT 5 Para Segurança da Informação

O modelo do COBIT 5 baseia-se em cinco princípios básicos, que são cobertos detalhadamente e incluem ampla orientação sobre os habilitadores de governança e gestão de TI da organização, entre eles o COBIT 5 for Information Security (Figura 02).

Figura 2 – Família de Produtos COBIT 5



Fonte: ISACA, COBIT 5, USA, 2012

Construído com base na estrutura do COBIT 5, para oferecer um guia prático em segurança da informação em todos os níveis das organizações, esse guia foi lançado em 2012.

O guia ajuda as companhias a reduzir seus perfis de risco através da administração adequada da segurança. As informação e tecnologias correlatas são cada dia mais essenciais para as organizações, mas a segurança da informação é essencial para a confiança dos acionistas. Este é o guia mais completo e atualizado e que incorpora o COBIT com aspectos de muitos padrões e práticas bem aceitos globalmente na atualidade. Não é apenas útil para profissionais de segurança, mas para negócios e usuários de TI em geral. Ainda aqueles que não se consideram profissionais de segurança irão perceber que os apêndices oferecem ótimas informações detalhadas de segurança em cada um dos sete habilitadores que são simples de entender e são bastantes úteis.

1.5.3.1 Princípios de Governança do COBIT 5 relacionados à Segurança da Informação

Conforme podemos observar na figura 3, o framework define cinco princípios básicos para governança e gestão da TI:

Figura 3 – Princípios do COBIT 5

Fonte: ISACA, COBIT 5, USA, 2012

1. Atender às Necessidades das Partes Interessadas

> De acordo com a tradução do COBIT 5, as organizações existem para criar valor para as partes interessadas – incluindo partes interessadas da segurança da informação – mantendo o equilíbrio entre a realização de benefícios e a otimização de risco e o uso dos recursos.

Como ferramenta de auxílio na adequação das necessidades das partes interessadas e dos diferentes e conflitantes objetivos, o framework COBIT 5 usa a Cascata de Objetivos (figura 4), na qual essas necessidades são traduzidas em objetivos corporativos – específicos e praticáveis –, em seguida, desdobrados em objetivos de TI e estes, consequentemente, desdobrados em metas de habilitadores, de forma adequada ao ambiente da organização, esses habilitadores compõem o último nível da cascata.

Figura 4 – Visão Geral da cascata de Objetivos do COBIT 5

Fonte: ISACA, COBIT 5, USA, 2012

A Segurança da Informação também compõe o conjunto de necessidade das partes interessadas (direcionadores). Aplicando-se a cascata neste caso, chega-se aos objetivos de segurança de informação corporativos e estes são desmembrados também em objetivos de TI que serão desmembrados em metas para os diferentes habilitadores.

2. Cobrir a Organização de Ponta a Ponta

Cobre todas as funções e processos corporativos; O COBIT 5 não se concentra somente na 'função de TI', mas considera a tecnologia da informação e tecnologias relacionadas como ativos que devem ser tratados como qualquer outro ativo por todos na organização.

> Considera todos os habilitadores de governança e gestão de TI aplicáveis à organização de ponta a ponta, ou seja, incluindo tudo e todos - interna e externamente - que forem considerados relevantes para a governança e a gestão das informações e de TI da organização. (ISACA, 2012. Tradução do autor).

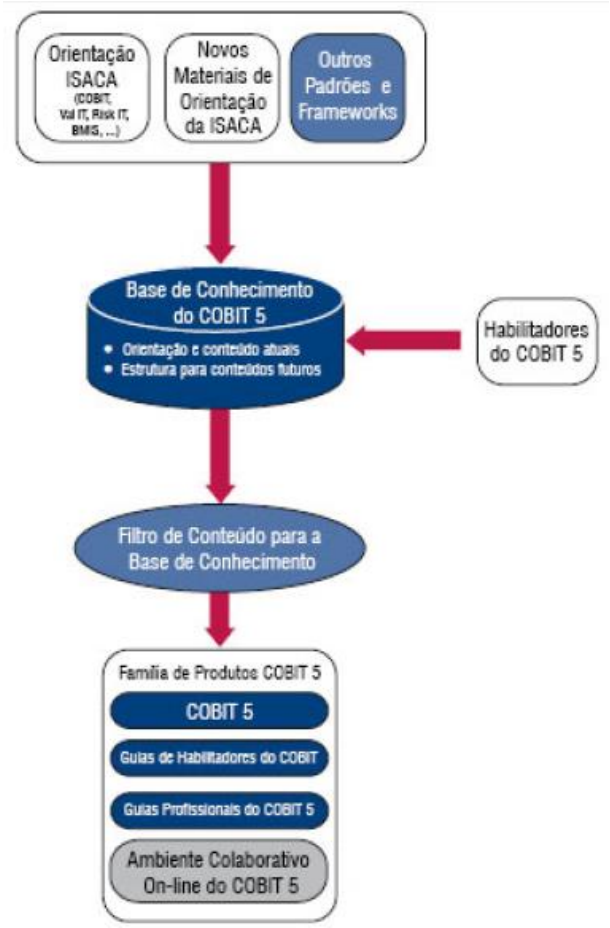
A aplicação deste princípio atende a todas as partes interessadas, funções e processos da organização que são relevantes para a segurança da informação.

3. Aplicar um Modelo Único Integrado

Neste princípio, o guia do COBIT 5 para Segurança da Informação, reúne, especificamente, conhecimentos de outros frameworks e orientações de importantes normas técnicas relacionadas à Segurança da Informação, já mencionados na introdução do capítulo.

Como um framework único e integrado, o COBIT 5 torna-se uma referência consistente de orientação com uma linguagem não técnica no diagnóstico comum do ambiente organizacional, permitindo o seu uso na governança e na gestão corporativa da TI. A figura 5 ilustra o mencionado modelo único e integrado.

Figura 5 – Modelo Único Integrado do COBIT 5



Fonte: ISACA, COBIT 5, USA, 2012

4. Permitir uma Abordagem Holística

> Governança e gestão eficiente e eficaz de TI da organização requer uma abordagem holística, levando em conta seus diversos componentes interligados. O COBIT 5 define um conjunto de habilitadores para apoiar a implementação de um sistema abrangente de governança e gestão de TI e informação da organização. (ISACA, 2012. Tradução do autor).

Neste princípio, o framework do COBIT 5 ressalta e define sete categorias de Habilitadores como sendo os vetores para maximização dos investimentos em tecnologia da informação e promovendo benefícios para as partes interessadas. Esses habilitadores estão descritos mais adiante neste capítulo, em Habilitadores.

5. Distinguir a Governança da Gestão

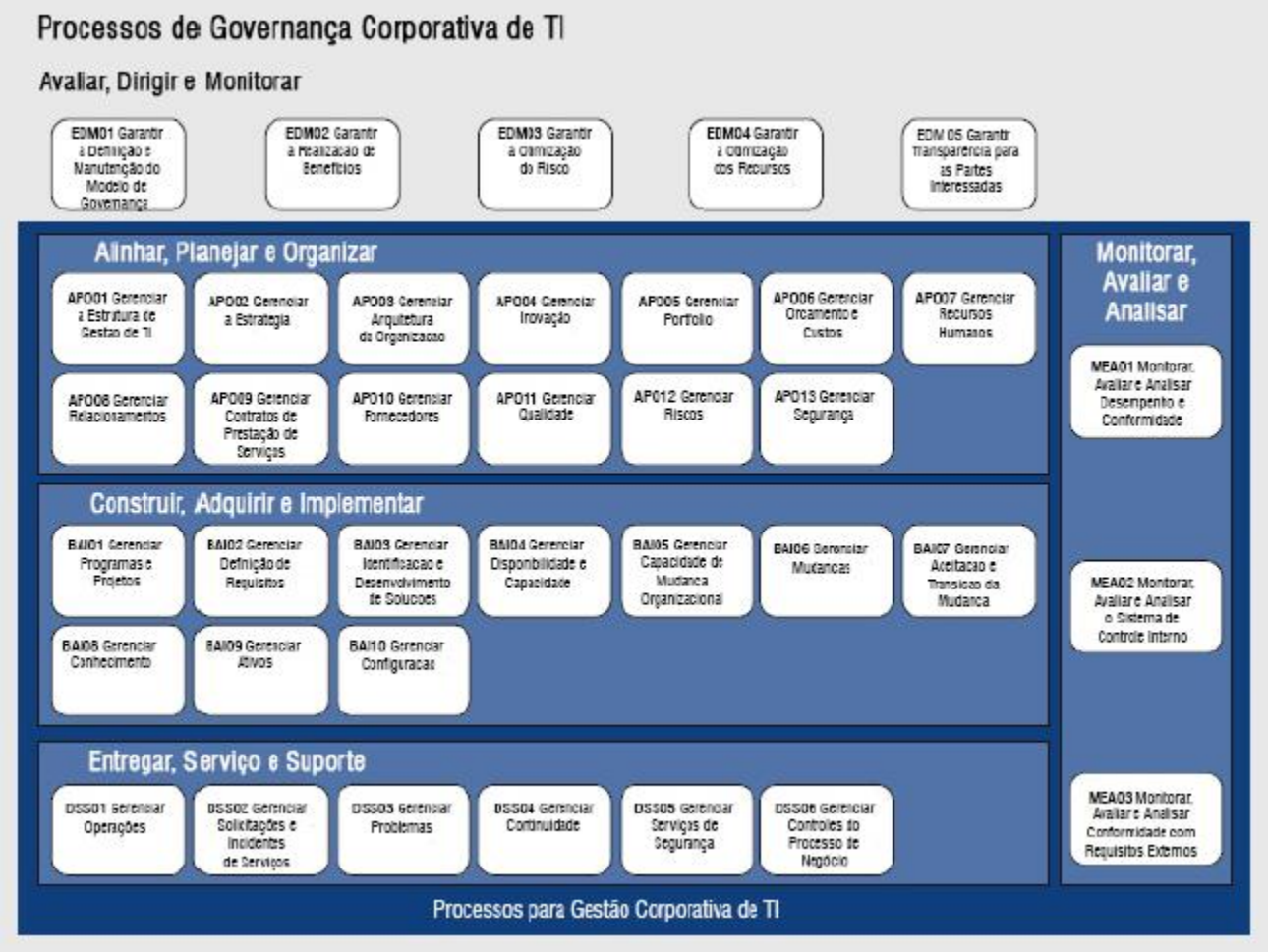
Em referência ao guia do COBIT 5 para Segurança da Informação, este aborda uma clara distinção entre governança e gestão. Essas duas funções abrangem diferentes tipos de atividades, envolvem diferentes estruturas organizacionais para atender os objetivos estratégicos, além de atender a propósitos distintos. A referida distinção entre governança e gestão é definida da seguinte forma:

> **Governança**: Garante que as necessidades, condições e opções das partes interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos. (ISACA, 2012. Tradução do autor).

> **Gestão**: É responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos. (ISACA, 2012. Tradução do autor).

O referido guia também ressalta que, na maioria das empresas, a governança é da responsabilidade do conselho de administração, sob a liderança do presidente e a gestão executiva está sob a liderança do diretor-presidente (CEO). Esses distintos papéis, governança da segurança da informação e gestão da segurança da informação, aparecem explicitamente no modelo de referência do COBIT 5 (figura 6) que inclui processos de governança e processos de gestão, ou seja, cada conjunto com as suas próprias responsabilidades.

Figura 6 – Modelo de Referência de Processo do COBIT 5



Fonte: ISACA, COBIT 5, USA, 2012

Estes princípios permitem que as organizações construam um modelo eficiente de governança e gestão de TI, otimizando os investimentos em TI e gerando benefícios para as partes interessadas. Por sua vez, o guia do COBIT 5 for Information Security também referencia os mesmos princípios, bem como a relevância de cada para a segurança da informação.

1.5.3.2 Habilitadores do COBIT 5 relacionados à Segurança da Informação

Conforme mencionado no 4º Princípio – Permitir uma Abordagem Holística, a segurança da informação está relacionada com todos os sete habilitadores, ilustrados na figura 7.

Figura 7 – Habilitadores Corporativos do COBIT 5

Fonte: ISACA, COBIT 5, USA, 2012

O guia para Segurança da Informação, descreve habilitadores como sendo fatores que, individual e coletivamente, influenciam se a governança e gestão vai funcionar em toda TI da organização com relação à governança de segurança da informação.

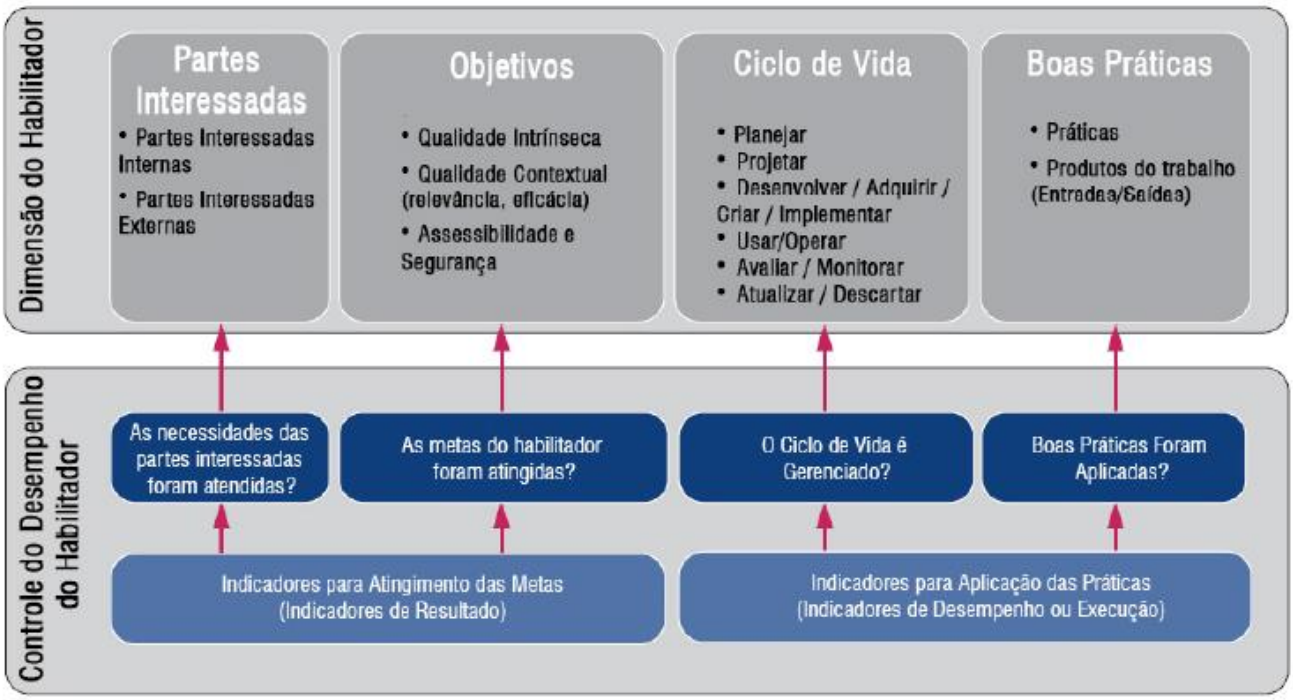
> Habilitadores são movidos por objetivos da cascata, ou seja, as metas de alto nível, relacionados a TI e definir o que os diferentes habilitadores devem alcançar. (ISACA. COBIT 5 for Information Security, 2012. Tradução do autor).

O COBIT 5 elucida os sete habilitadores, são eles:

1. Princípios, políticas e frameworks: São veículos para a tradução do comportamento desejado em orientações práticas para a gestão diária; inclui informações de segurança, princípios, políticas e frameworks.
2. Processos: Descrevem um conjunto organizado de práticas para alcançar determinados resultados para atingir os objetivos de TI; incluem detalhes e atividades específicas de segurança da informação.
3. Estruturas organizacionais: São as principais entidades de tomada de decisão de uma organização; inclui estruturas organizacionais específicas de segurança da informação.
4. Cultura, ética e comportamento: Está relacionado a pessoas e organizações que muitas das vezes são subestimados como um fator de sucesso nas atividades de governança e gestão; considera também os fatores que determinam o sucesso de governança e gestão da segurança da informação.

5. Informações: Permeia qualquer organização e inclui todas as informações produzidas e utilizadas pela organização. A Informação é necessária para manter a organização em funcionamento e bem governada. No nível operacional, a informação por si só é muitas vezes o principal produto da organização; inclui informações específicas da segurança da informação.
6. Serviços, infraestrutura e aplicativos: Incluem a infraestrutura, a tecnologia e os aplicativos que fornecem à organização o processamento e os serviços de TI necessários; inclui também serviços específicos para suportar a segurança da informação nas organizações.
7. Pessoas, habilidades e competências: Estão associadas às pessoas e são necessárias para a conclusão bem-sucedida de todas as atividades, bem como para a tomada de decisões corretas e medidas corretivas.

Figura 8 – Habilitadores do COBIT 5: Genéricos



Fonte: ISACA, COBIT 5, USA, 2012

Reforçando a importância desses habilitadores, é possível afirmar que podem ser aplicados em situações práticas nas empresas, bem como serem usados para implementar a governança e a gestão da segurança da informação, conforme o modelo genérico do COBIT 5 (figura 8). Esse modelo demonstra a estrutura do conjunto de Dimensões comum a todos os habilitadores, de forma simples, efetiva e eficiente, para atingir os resultados desejados, inclusive na implementação da segurança da informação.

As Dimensões dos habilitadores são:

- ✓ Partes interessadas
  - Todo habilitador possui partes interessadas internas e externas à organização.
- ✓ Objetivos/metas
  - Diversas metas para cada habilitador que criam valor ao atingi-las; podem ser divididas em Qualidade intrínseca, Qualidade contextual e Acesso e Segurança.
- ✓ Ciclo de Vida
  - O habilitador inclui a criação, vida útil operacional e descarte.
- ✓ Boas Práticas
  - Apoiam as metas dos habilitadores; fornece exemplo de como implementar o habilitador; entre outros.

Conforme ilustrado na figura 8, além das quatro dimensões de habilitadores, o COBIT 5 orienta como controlar o desempenho dos habilitadores de forma específica – considera perguntas e respostas pré-definidas, bem como os indicadores de resultados e indicadores de progresso. Em relação aos indicadores, o de resultados serve para aferir se as metas dos habilitadores foram alcançadas. O indicador de performance refere-se ao efetivo funcionamento dos habilitadores.

1.5.3.3 Iniciativas de Implantação da Segurança da Informação

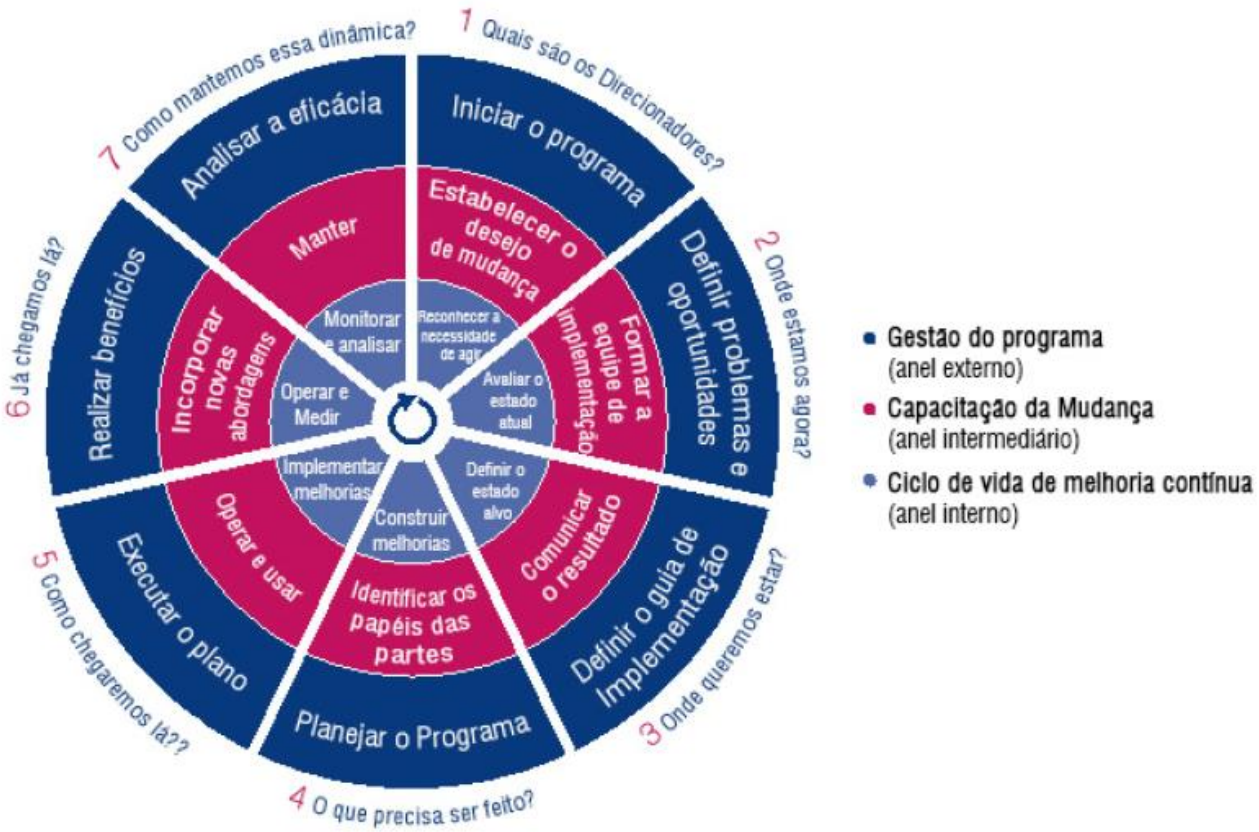
O guia COBIT 5 para Segurança da Informação, considera que as organizações necessitam definir seus próprios habilitadores para implantação da segurança da informação, bem como os fatores internos e/ou externos no ambiente no qual está inserida, tais como:

- ✓ Ética e cultura para segurança da informação
- ✓ Leis, regulamentos e políticas
- ✓ Regulamentações contratuais aplicáveis
- ✓ Políticas e práticas existentes
- ✓ O nível de maturidade dos facilitadores de segurança da informação atual
- ✓ Capacidades de segurança da informação e os recursos disponíveis
- ✓ Práticas da indústria
- ✓ Padrões e estruturas obrigatórias sobre segurança da informação

Deve considerar também a definição dos requisitos de segurança da informação da organização, tendo como base o plano de negócios, o seu modelo de gestão, o perfil de risco da informação e o seu apetite ao risco. Além disso, os frameworks de melhores práticas e padrões são úteis apenas se forem adotados e adaptados de forma assertiva porque existem desafios que precisam ser superados e problemas que precisam ser resolvidos para que a gestão estratégica de TI seja implantada com êxito, além de fornecer orientações de como fazer.

Para as iniciativas de implementação da segurança da informação, o guia COBIT 5 para Segurança da Informação ilustra um modelo próprio, denominado os três componentes inter-relacionados do ciclo de vida da implementação, cujo objetivo é de tratar a complexidade e os desafios encontrados nessas iniciativas, considerando também os ambientes disponíveis e adequados nas organizações. O mencionado modelo, possui sete fases de implementação e estão agrupadas em três estágios: Gestão do Programa (anel externo), Capacitação da Mudança (anel intermediário) e Ciclo de Vida de Melhora Contínua (anel interno), conforme figura 9.

Figura 9 – As Sete Fases do Ciclo de Vida da Implementação



Fonte: ISACA, COBIT 5, USA, 2012

As sete fases do ciclo de vida da implementação, são:

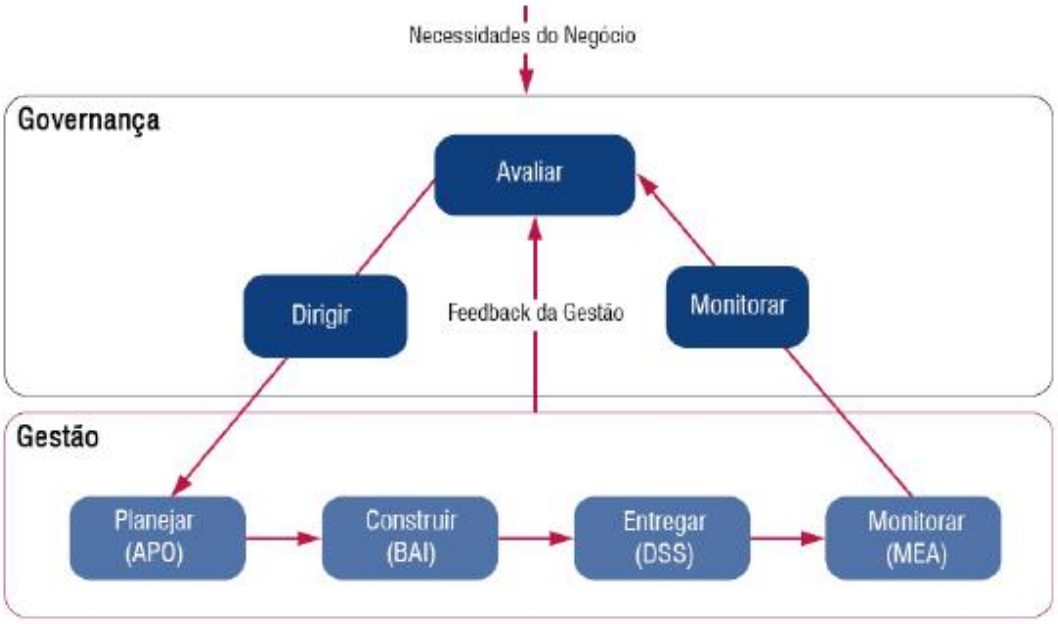
1. Quais são os Direcionadores?
2. Onde estamos agora?
3. Onde queremos estar?
4. O que precisa ser feito?
5. Como chegaremos lá?
6. Chegamos lá?
7. Como manter o impulso?

Apesar de não estarem detalhadas, é possível obter todas as informações no framework do COBIT 5. É importante mencionar que todas as fases possuem relevância na implementação das iniciativas, sejam relativas à segurança da informação ou não. Entretanto, na implantação da segurança da informação, observa-se que as fases 1, 2, e 3 abordam escopos específicos e orientações relacionados aos habilitadores.

1.5.3.4 Processos de Gestão da Segurança da Informação

O COBIT 5 não é prescritivo, mas defende que as organizações implementem os processos de governança e gestão de tal forma que as principais áreas sejam cobertas, conforme demonstrado na figura 10.

Figura 10 – Principais Área de Governança do COBIT 5



Fonte: ISACA, COBIT 5, USA, 2012

Assim como o framework COBIT 5, o guia para Segurança da Informação também define três processos específicos para Gestão da Segurança da Informação:

- APO13 - Gerenciar a Segurança da Informação
    - Exige que um Sistema de Gestão de Segurança da Informação seja implementado para coordenar e gerir de forma eficaz e eficiente os recursos e processos utilizados, e os controles necessários para garantir confidencialidade, integridade e disponibilidade dos sistemas de informação alinhado com os objetivos operacionais e estratégicos predefinidos.
- DSS04 – Gerenciar Continuidade
    - Estabelece e mantém um plano para permitir o negócio e TI responder a incidentes e interrupções, a fim de continuar a operação de processos críticos de negócios e serviços de TI necessários e mantém a disponibilidade de informações em um nível aceitável para a organização.
- DSS05 - Gerenciar Serviços de Segurança da Informação
    - Protege informações da organização para manter o nível de risco aceitável para a segurança da informação da organização, de acordo com a política de segurança. Estabelece e mantém as funções de segurança da informação e privilégios de acesso e realiza o monitoramento de segurança.

2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

2.1 Definição de Política de Segurança da Informação e Comunicação

Política de segurança é uma declaração formal das regras que devem ser obedecidas pelas pessoas que tem acesso à tecnologia e às informações da empresa – Security HandBook (RFC2196). Uma política de segurança é basicamente um manual de procedimentos que descreve como os recursos que manipulam as informações da empresa devem ser protegidos e utilizados, e é o pilar da eficácia da Segurança da Informação, estabelecendo investimentos em recursos humanos e tecnológicos (CASTRO, 2002).

Uma política de segurança é a formalização de todos os aspectos considerados relevantes por uma organização para a proteção, controle e monitoramento de seus recursos computacionais e, consequentemente, das informações por eles manipuladas. Em outras palavras, uma forma mais prática, a política de segurança deve contemplar, de forma genérica, todos os aspectos importantes para a proteção lógica e física das informações e dos recursos computacionais.

Segundo Sousa (2006) o desenvolvimento de uma política de segurança é a base de segurança de informação em uma empresa. Alguns padrões e normas internacionais de segurança foram desenvolvidos por organizações normalizadoras como ISO (Internacional Standards Organization) e a BS (British Standard), como ISO 27002 e a BS 7799.

Na perspectiva de Marciano (2006) uma política de segurança da informação é um conjunto de regras, normas e procedimentos que regulam como deve ser gerenciada e protegida a informação sensível, assim classificada pela organização ou pelo estado, além dos recursos e utilizadores que com ela interagem. Todo o ciclo de vida da informação deve ser objeto da política.

Conforme Campos (2006) citado por Sierwert (s/d) uma política de segurança não é um grande livro informando tudo o pode existir de segurança da informação dentro de uma corporação ou instituição, nem mesmo são poucas regras gerais que se aplicam a qualquer aspecto da segurança da informação. Ainda que essas duas hipóteses não

possam ser descartadas, nenhuma delas define exatamente o que é uma política de segurança da informação.

> Mas afinal de contas o que significa a palavra política, que atualmente está sendo tão utilizada pelas corporações e instituições? Atualmente é comum ouvir frases do tipo “a política da nossa empresa é a qualidade total de nossos produtos”, ou então “a política de recursos humanos não tolera funcionários que tenham registro policial”. Esses são dois exemplos, mas que ajudam a entender o que significa a palavra política. A primeira frase é bastante abrangente e qualquer procedimento, ação ou decisão visando como objetivo a qualidade dos produtos fabricados, está de acordo com a política estabelecida pela empresa. Já a segunda frase é mais específica e deve ser considerada no processo de seleção e recrutamento de funcionários da empresa, conforme estabelecido na política de recursos humanos da empresa. (CAMPOS, 2006 apud SIERWERT, 2006).

Com a política de segurança não é diferente, ou seja, ela deve indicar como as coisas devem acontecer na organização ao que se refere a segurança da informação, sendo assim, uma política nada mais é do que um conjunto de regras que determina como deve ser o comportamento de pessoas que tem qualquer tipo de relacionamento com a organização no que diz respeito as informações que são trocadas, enviadas ou recebidas. (CAMPOS, 2006).

No que diz respeito às políticas de segurança da informação, existe ainda um requisito a mais a ser cumprido: prover o equilíbrio entre funcionalidade e segurança, motivo pelo qual torna-se essencial uma análise da situação operacional da organização em foco. Esta análise, que no contexto da segurança da informação é conhecida como análise de vulnerabilidades, deve se restringir, como é de hábito, a uma busca por eventuais brechas de segurança nos sistemas de informação sobre os quais se aplica. Antes, deve-se conhecer a fundo os fluxos de informação aplicados (formais e informais) a fim de mapear-se de modo consistente e dinâmico a realidade, em termos da informação e dos atores que com ela interagem. (MARCIANO, 2006).

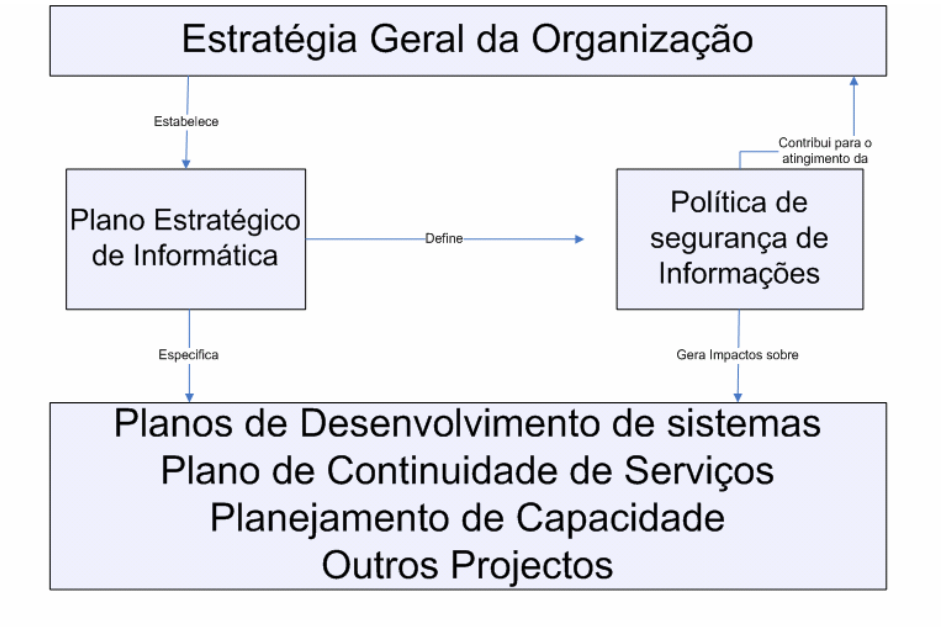
A política de segurança de informações deve estabelecer princípios institucionais de como a organização irá proteger, controlar e monitorar seus recursos computacionais e, consequentemente, as informações por eles manipuladas. É importante que a política estabeleça ainda as responsabilidades das funções relacionadas com a segurança e discrimine as principais ameaças, riscos e impactos envolvidos. (DIAS, 2000 apud LAUREANO, 2005).

Ainda referindo ao mesmo autor Dias (2000) citado por Laureano (2005) salienta que a política de segurança, deve ir além dos aspectos relacionados com sistemas de

informação ou recursos computacionais, ela deve estar integrada as políticas institucionais da empresa, metas de negócio e ao planejamento estratégico da empresa.

A figura 11 mostra o relacionamento da política de segurança de informações com a estratégia da organização, o plano estratégico de informática e os diversos projetos relacionados. (DIAS, 2000 apud LAUREANO, 2005).

Figura 11 - Princípios de Governança da Segurança da Informação



Fonte: Laureano (2005)

2.2 Características de uma Política de Segurança da Informação e Comunicação

Conforme exposto por Ferreira (2006), uma política e segurança da informação não deve ser elaborada se não tiver as seguintes características:

a) De fácil leitura e entendimento;
b) Compreensível, ou seja, escrita de maneira clara e objetiva;
c) Homologada e assinada pela Alta Administração;
d) Estruturada, estabelecendo padrões;
e) Alinhada com a estratégia da missão da organização;
f) Orientada aos riscos, ou seja, direcionar para os riscos da organização;
g) Flexível, ou seja, moldáveis aos novos requerimentos de tecnologia;
h) Protetora dos ativos de informação, priorizando os de maior valor e de maior importância;
i) Positiva e não apenas concentradas em ações proibitivas ou punitivas;

j) Deve conter atribuições de regras e responsabilidades;
k) Deve conter a forma de educar os usuários;
l) Deve ser dinâmica, ser atualizada sempre que necessário;
m) Deve ser acessível a todos; e
n) Deve ser exequível, ou seja, descreva regras de comportamentos que possam ser cumpridas, fáceis de executar, sejam na área tecnológica ou humana.

Por meio das afirmações de Ferreira (2006), podemos entender que uma política de segurança da informação e comunicação somente pode ser implementada com o apoio da alta administração da organização e para que esta política seja efetiva, todas as diretrizes, objetivos e metas devem estar de forma clara, transparente e sucinta, de forma que qualquer pessoa da organização possa compreender e aplicar nas suas atividades. Por oportuno, é interessante destacar que esta política de segurança da informação e comunicação deve ser revista periodicamente a fim de que este documento acompanhe as atualizações tecnológicas e mudanças procedimentais quando ocorrerem.

Segundo Spanceski (2004) os controles considerados como melhores práticas para a segurança da informação incluem:

- ✓ Documentação da política de segurança da informação;
- ✓ Definição das responsabilidades na segurança da informação;
- ✓ Educação e treinamento em segurança da informação;
- ✓ Relatório de incidentes de segurança;
- ✓ Gestão de continuidade do negócio.

Contudo, em Lyra (2015), o sucesso da POSIC está diretamente relacionado com o envolvimento e a atuação da alta administração. Quanto maior for o comprometimento da gerência superior com os processos de elaboração e implantação da POSIC, maior a probabilidade de ela ser efetiva e eficaz.

2.3 Tipos de Política de Segurança da Informação e Comunicação

Segundo Spanceski (2004) existem três tipos de políticas entres quais a refutatória, consultiva e a informativa.

2.3.1 Refutatória

Na óptica de Ferreira (2003) citado por Spanceski (2004) afirma que políticas refutatórias são implementadas devido às necessidades legais que são impostas à organização. Normalmente são muito específicas para um tipo de ramo de atividade.

Em relação ao mesmo autor uma política refutatória é definida como se fosse uma série de especificações legais. Descreve, com grande riqueza de detalhes, o que deve ser feito, quem deve fazer e fornecer algum tipo de parecer, relatando qual ação é importante. (FERREIRA, 2003 apud SPANCESKI, 2004).

2.3.2 Consultiva

Segundo Spanceski (2004) políticas consultivas não são obrigatórias, mas muito recomendadas. As organizações devem conscientizar seus funcionários a considerar este tipo de política como se fosse obrigatória.

A política consultiva apenas sugere quais ações ou métodos devem ser utilizados para a realização de uma tarefa. A ideia principal é esclarecer as atividades quotidianas do dia-a-dia da empresa de maneira bastante direta. (SPANCESKI, 2004).

No entender de Ferreira (2003) citado por Spanceski (2004) deve-se considerar que é importante que os utilizadores conheçam essas ações para realização de suas tarefas para que possam ser evitados riscos do não cumprimento das mesmas, tais como:

- ✓ Possibilidade de omissão de informações importantes para tomada de decisões críticas aos negócios da organização;
- ✓ Falhas no processo de comunicação com a alta administração;
- ✓ Perda de prazos de compromissos importantes para os negócios da organização.

2.3.3 Informativa

Este tipo de política possui carácter apenas informativo, nenhuma ação é desejada e não existem riscos, caso não seja cumprida. Porém, também pode contemplar uma série

de observações importantes, bem como advertências severas. (FERREIRA, 2003 apud SPANCESKI, 2004)

Por exemplo, a política pode ressaltar que o uso de um determinado sistema é restrito a pessoas autorizadas e qualquer funcionário que realizar algum tipo de violação será penalizado. Nesta sentença não são informados quais funcionários estão autorizados, mas este determinando severas consequências para quem desrespeita-la. (FERREIRA, 2003 apud SPANCESKI, 2004)

Na óptica de Ortalo (1996) citado por Marciano (2006), os elementos principais de uma política de segurança da informação são os seguintes:

Elementos básicos, os quais descrevem os diferentes indivíduos, objetos, direitos de acesso e atributos presentes na organização ou no sistema, e que definem o vocabulário segundo o qual a política é construída;

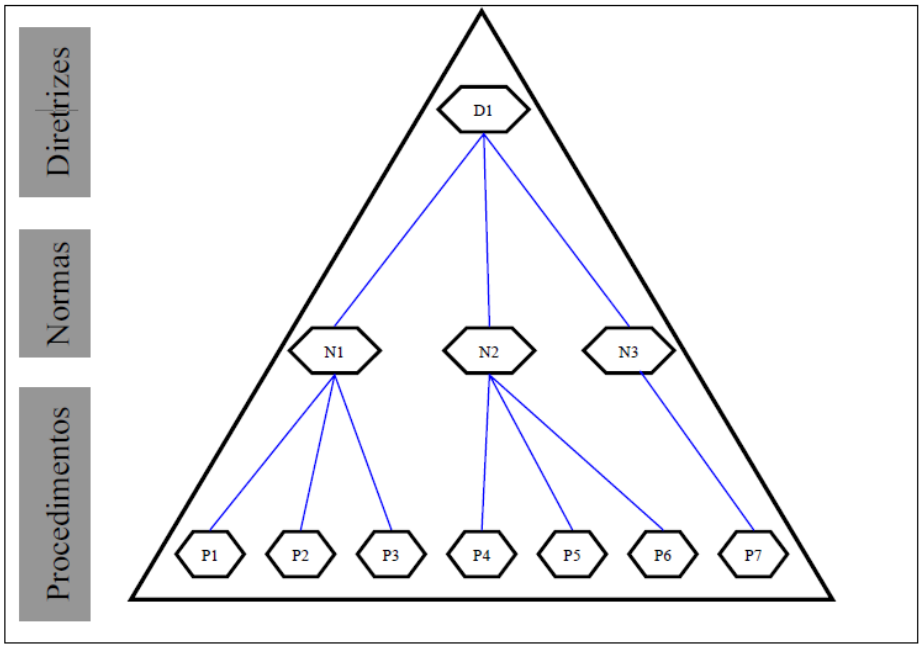
Os objetivos da segurança, ou seja, as propriedades desejadas do sistema com respeito à segurança, definida em termos dos atributos desta (confidencialidade, integridade e disponibilidade);

Um esquema de autorização, na forma de um conjunto de regras descrevendo os mecanismos do sistema relevantes à segurança, com a descrição das eventuais modificações no estado da segurança.

2.4 Elaborando uma Política de Segurança da Informação e Comunicação

Conforme Campos (2006), não existe uma regra para criar o documento físico da política de segurança. É possível ter um documento único com as diretrizes, normas e procedimentos, ou um documento com as diretrizes, diversos outros com as normas e vários outros com os demais procedimentos. O fato principal é que as diretrizes, normas e procedimentos têm que existir em um documento com controle de versão e com revisão para garantir que sejam confiáveis e relevantes. A visão conceitual de uma política de segurança da informação e comunicação é apresentada na figura 12.

Figura 12 - Visão conceitual da política de segurança



Fonte: Adaptado de Campos (2006)

Na figura 12, é destacada a relação entre diretrizes, normas e procedimentos, ou seja, um objeto depende do outro, se existir algum procedimento que não tem relacionamento com nenhuma norma, e alguma norma não tiver relacionamento com alguma diretriz, então a política de segurança está com algo errado, e deve ser revista.

De acordo com Silva (2004), a política de segurança deve ir além dos aspectos de sistemas de informação e recursos computacionais, integrando as políticas institucionais relativas à segurança em geral, às metas de negócios da organização e ao plano estratégico de informática. O objetivo da POSIC é atingido quando o relacionamento da estratégia da organização, o plano estratégico de informática e demais projetos estiverem sincronizados.

2.5 Princípios que norteiam uma Política de Segurança da Informação e Comunicação

A correta gestão da segurança da informação é atingida com o compromisso de todos os usuários quanto à aplicação das normas e procedimentos estabelecidos visando

à padronização das ações de planeamento, implementação e avaliação das atividades voltadas à segurança. (WILIAMS, 2001 apud MARCIANO, 2006).

Estas diferentes atividades podem ser agrupadas conforme a disposição da Information Systems Audit and Control Foundation (ISACF, 2001 apud MARCIANO, 2006):

- ✓ Desenvolvimento de políticas, com os objetivos da segurança como fundamentos em torno dos quais elas são desenvolvidas;
- ✓ Papéis e autoridades, assegurando que cada responsabilidade seja claramente entendida por todos;
- ✓ Delineamento, desenvolvendo um modelo que consista em padrões, medidas, práticas e procedimentos;
- ✓ Implementação, em um tempo hábil e com capacidade de manutenção;
- ✓ Monitoramento, com o estabelecimento de medidas capazes de detectar e garantir correções às falhas de segurança, com a pronta identificação e atuação sobre falhas reais e suspeitas com plena aderência à política, aos padrões e às práticas aceitáveis;
- ✓ Vigilância, treinamento e educação relativos à proteção, operação e prática das medidas voltadas à segurança.

2.6 Aspectos que contemplam uma Política de Segurança da Informação e Comunicação

De acordo com Ferreira (2003), em seu livro Segurança da Informação, os aspectos que contemplam uma Política de Segurança da Informação e Comunicação são:

a) Especificação da política: A política deve ser breve, utilizar palavras simples e formalizar o que é esperado dos servidores da organização. Deve fornecer informações suficientes para saber se os procedimentos descritos na política são aplicáveis para eles ou não. Deve descrever sua finalidade específica, ou seja, se é orientada a pessoa, departamentos e/ou equipamentos;

b) Declaração da Alta administração: Uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação. Esta formalização demonstra aos servidores que a alta autoridade mostra seu comprometimento para que a política de segurança da informação seja adequadamente cumprida;

c) Autores/patrocinadores da política: Os nomes dos profissionais ou equipes, que desenvolveram a política devem estar especificados no documento;

d) Fazer referência a outras políticas, regulamentos ou regimentos: Em organizações é comum que as políticas de segurança em vigor façam referência a outros regulamentos internos já existentes;
e) Procedimentos para requisição de exceção à política: É importante preparar e divulgar a política, mas também é essencial ter um processo para requisição de exceção a ela;
f) Procedimentos para mudanças da política: Algumas organizações não atualizam suas políticas, sendo assim, é necessário ter um procedimento para atualização dela. Há situações que podem requerer somente revisões técnicas, mas outras necessitarão de justificativas detalhadas para solicitar mudanças nas políticas;
g) Punições para àqueles que violarem a política: A alta administração deve demonstrar que poderão ocorrer punições rígidas aos servidores da organização caso haja um desrespeito ou violarem as políticas internas;
h) Data de publicação, validade e revisão da política: A política e seus documentos complementares devem possuir assinatura do principal executivo, data da última atualização e do início de sua vigência.

2.7 Política de Segurança da Informação segundo a NBR ISO 27002:2013

2.7.1 Política de Segurança da Informação

Segundo a NBR ISO/IEC 27002:2013, a norma tem como objetivo prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

A Política de Segurança da Informação é essencialmente um manual de procedimentos que descreve como os recursos que manipulam as informações das empresas devem ser protegidos e utilizados, e é o pilar da eficácia da Segurança da Informação, estabelecendo investimentos em recursos humanos e tecnológicos. (LYRA, 2015)

2.7.2 Documento da Política de Segurança da Informação

Ainda segundo a NBR ISO/IEC 27002:2013, é prudente que um conjunto de políticas de segurança da informação e comunicação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. É importante destacar que no mais alto nível, a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.

É prudente que as POSIC contemplem requisitos oriundos de:

a) Estratégia do negócio;
b) Regulamentações, legislação e contratos;
c) Ambiente de ameaça da segurança da informação, atual e futuro.

Também é conveniente que a POSIC contenha declarações relativas a:

a) Definição de segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
b) Atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;
c) Processos para o tratamento dos desvios e exceções.

No nível mais baixo, convém que a política da segurança da informação seja apoiada por políticas específicas do tema, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.

É muito importante que estas políticas sejam comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de “um programa de conscientização, educação e treinamento em segurança da informação. ”

2.7.3 Análise Crítica da Política de Segurança da Informação

Segundo a ISO/IEC 27002:2013, é conveniente que as políticas de segurança da informação e comunicação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequada e eficácia. Esta análise de maneira critica visa o aperfeiçoamento da política, de

forma que possamos reavaliar o seu planejamento, os seus controles assim como analisar os incidentes de segurança da informação que ocorreram no período. E, por fim, verificar se a há novas ameaças e vulnerabilidades, de forma que política atenda plenamente aos objetivos da organização com a constante evolução tecnológica.

2.8 Utilizando o COBIT 5 for Information Security para otimizar a POSIC

O COBIT 5 oferece um quadro abrangente que auxilia as empresas a atingir os seus objetivos para a Governança Corporativa de TI, isso ajuda as empresas a criar o valor ideal de tecnologia da informação criando um equilíbrio entre a percepção dos benefícios e a otimização dos níveis de risco e a utilização de recursos. O framework permite que as empresas sejam governadas e geridas de uma forma holística, tendo em conta o negócio fim a fim, considerando os interesses relacionados com a TI e dos stakeholder internos e externos.

O COBIT 5 para Segurança da Informação, já detalhado no capítulo anterior, é baseado no framework COBIT 5 na medida em que se concentra na segurança da informação e fornece orientações mais detalhadas e mais prático para os profissionais de segurança da informação e outras partes interessadas em todos os níveis da empresa.

2.8.1 Princípios da Segurança da Informação

Conforme apresentados e consolidados na Figura 5 abaixo, que poderiam direcionar a construção de políticas de segurança da informação de forma a agregar valor as instituições mantenedoras de forma não apenas tática e normatizada, mas também alinhando e considerando as necessidades estratégicas do negócio como ponto fundamental em uma política de segurança (SOUZA NETO, 2012).

Os Princípios de Segurança da Informação têm a finalidade de comunicar as regras da empresa em apoio aos objetivos de governança e valores corporativos definidos pelo conselho de administração e gestão executiva. Estes princípios devem ser:

- ✓ Em número limitado;
- ✓ Expresso em linguagem simples, o mais claro possível.

Em 2010, as três principais organizações globais de segurança da informação - ISACA, ISF e International Information System Security Certification Consortium [(ISC)²] –

uniram suas forças e montaram um consórcio para desenvolver 12 princípios independentes, não-proprietários com a finalidade de ajudar os profissionais de segurança da informação agregar valor às suas organizações, apoiar com sucesso o negócio e promover práticas da boa segurança da informação.

Esses princípios foram produzidos para fornecer aos profissionais de segurança da informação um conjunto de regras que regem o comportamento, objetivos, abordagens e atividades, a fim de promover as boas práticas em segurança da informação.

Segundo John Colley, diretor executivo da (ISC) ², a profissão de segurança precisa romper suas raízes como uma disciplina focada em TI. Embora muitas organizações possua um código de ética ou valores orientadores para a sua adesão, o conjunto de princípios oferece aos profissionais orientação prática sobre como apoiar os objetivos de negócios.

Os 12 princípios são motivados por risco, governança e maior conformidade regulatória, e de acordo o consórcio, irão ajudar os profissionais de segurança a responder mais eficazmente às novas necessidades das complexas organizações no mundo interconectado de hoje. Por exemplo:

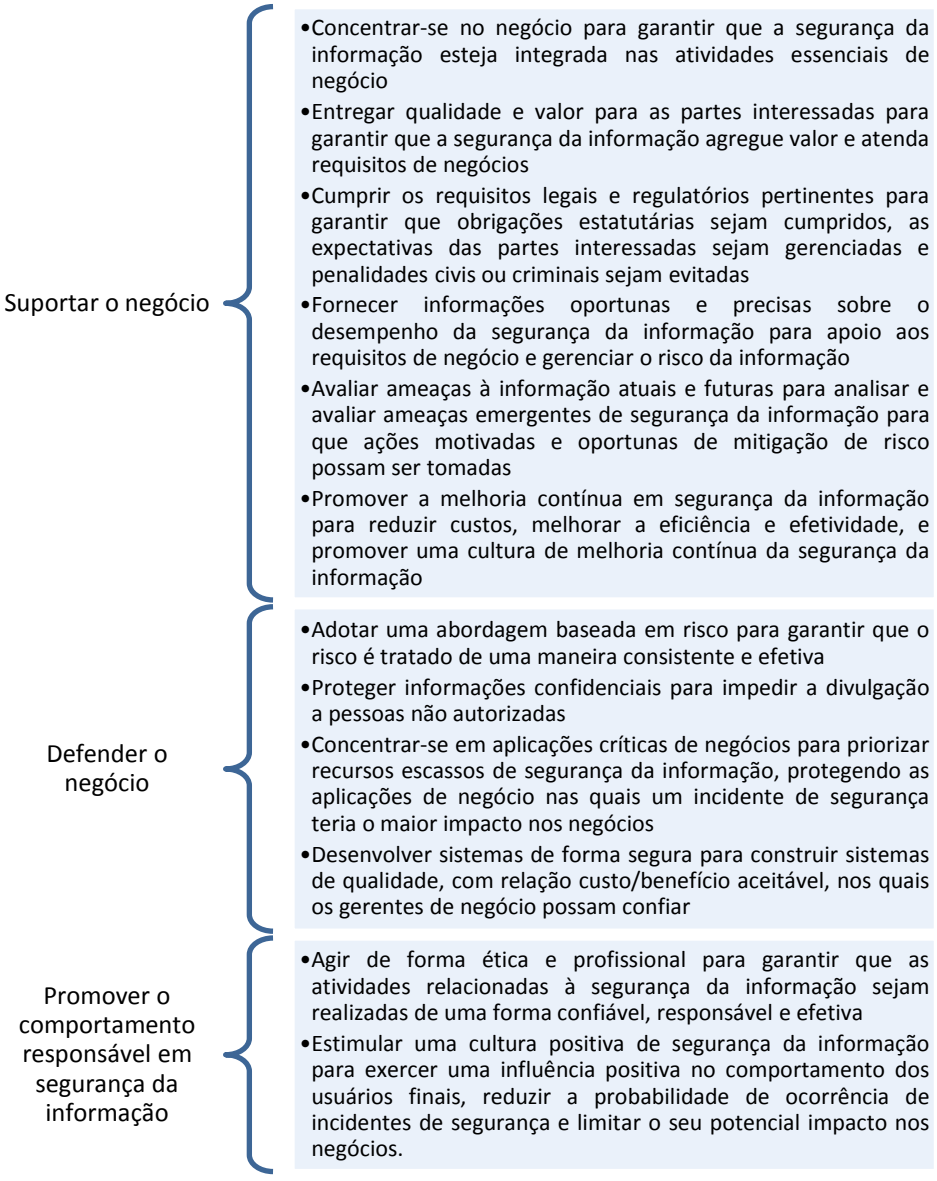
- A profissão de segurança da informação não está totalmente madura, tradicionalmente, tem um viés em relação à tecnologia da informação e precisa ser mais focada em riscos.
- Ameaças que evoluem rapidamente requerem profissionais de segurança da informação para ficar à frente da defesa.
- São necessários esforços coordenados para manter a capacidade de adaptação dos profissionais de segurança da informação, particularmente na mudança dos ambientes de negócios.

Ao longo dos anos tem havido um número de ofertas relacionadas com os profissionais de segurança da informação que cobrem comportamento, ações ou ética. No entanto, é um requisito para um conjunto independente, não-proprietário de princípios, que são:

- Mais genérico e completo, com menos foco em qualificação profissional;
- Relevantes para o mundo dos negócios;
- Aceito em toda a profissão de segurança, em vez de ser proprietária de uma organização;
- Capaz de mapear facilmente as diferentes normas e orientações de segurança.

Os 12 princípios para os profissionais de segurança da informação foram concebidos para atender a essas necessidades e estão estruturados em apoio das seguintes tarefas:

Figura 13 – Princípios de Segurança da Informação

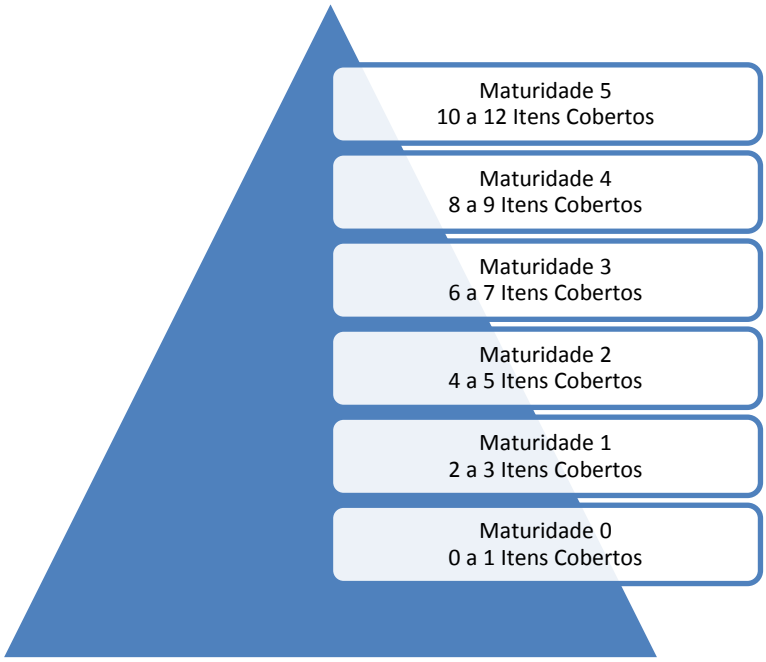


Fonte: Elaborado pelo autor (2015)

Uma vez familiarizado com esse conteúdo, foi feito uma análise de quais princípios nos documentos estariam em aderência com os 12 princípios da Governança da

Segurança da Informação propostos pelo ISACA, ISF e International Information System Security Certification Consortium, conforme figura 13 e classificamos os resultados da quantidade de princípios cobertos de acordo com a tabela de maturidade proposta na figura 14.

Figura 14 – Princípios de Segurança da Informação

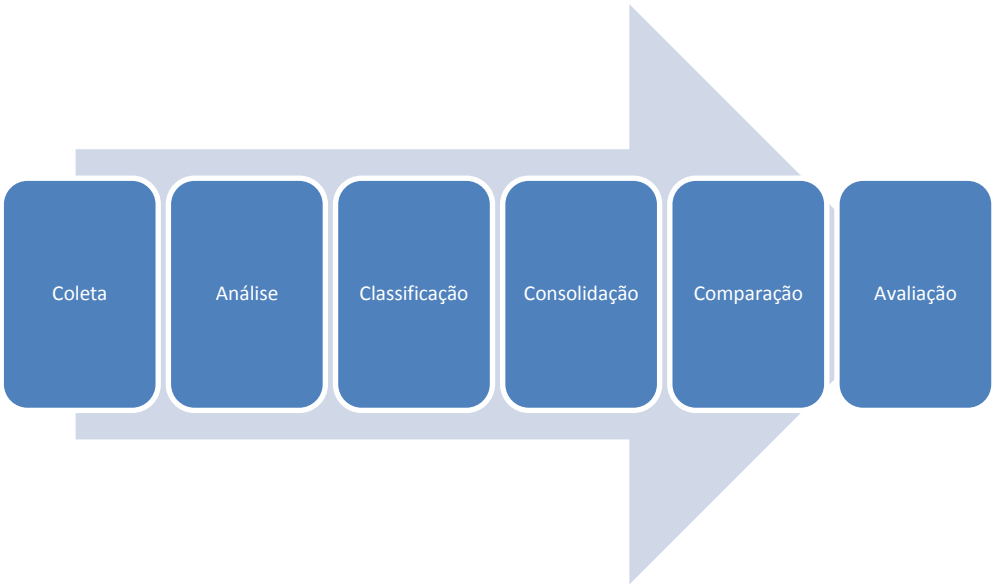


Fonte: Elaborado pelo autor (2015)

Após a coleta e classificação dos dados, foi realizada consolidação destes dados de forma comparar o nível de maturidade de cada órgão em relação a outro, bem como quais são os princípios mais cobertos e os menos cobertos e por fim uma análise comparativa com o modelo ISO 27002.

O processo completo pode ser observado na figura 15.

Figura 15 – Processo de Consolidação dos dados



Fonte: Elaborado pelo autor (2015)

Para efeito da classificação dos órgãos, será utilizado o código atribuído a cada princípio na tabela descritas abaixo, de forma a simplificar o processo.

Quadro 1 – Códigos dos Princípios de Suportar ao Negocio

Suportar o negócio	Concentrar-se no negócio para garantir que a segurança da informação esteja integrada nas atividades essenciais de negócio;	SN01
Suportar o negócio	Entregar qualidade e valor para as partes interessadas para garantir que a segurança da informação agregue valor e atenda requisitos de negócios	SN02
Suportar o negócio	Cumprir os requisitos legais e regulatórios pertinentes para garantir que obrigações estatutárias sejam cumpridos, as expectativas das partes interessadas sejam gerenciadas e penalidades civis ou criminais sejam evitadas	SN03
Suportar o negócio	Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação para apoio aos requisitos de negócio e gerenciar o risco da informação	SN04
Suportar o negócio	Avaliar ameaças à informação atuais e futuras para analisar e avaliar ameaças emergentes de segurança da informação para que ações motivadas e oportunas de mitigação de risco possam ser tomadas	SN05

Suportar o negócio	Promover a melhoria contínua em segurança da informação para reduzir custos, melhorar a eficiência e efetividade, e promover uma cultura de melhoria contínua da segurança da informação	SN06

Fonte: Elaborado pelo autor (2015)

Quadro 2 – Códigos dos Princípios de Defender o Negocio

Defender o negócio	Adotar uma abordagem baseada em risco para garantir que o risco é tratado de uma maneira consistente e efetiva	DN01
Defender o negócio	Proteger informações confidenciais para impedir a divulgação a pessoas não autorizadas	DN02
Defender o negócio	Concentrar-se em aplicações críticas de negócios para priorizar recursos escassos de segurança da informação, protegendo as aplicações de negócio nas quais um incidente de segurança teria o maior impacto nos negócios	DN03
Defender o negócio	Desenvolver sistemas de forma segura para construir sistemas de qualidade, com relação custo/benefício aceitável, nos quais os gerentes de negócio possam confiar	DN04

Fonte: Elaborado pelo autor (2015)

Quadro 3 – Códigos do Princípios de Promover o Comportamento

Promover o comportamento responsável em segurança da informação	Agir de forma ética e profissional para garantir que as atividades relacionadas à segurança da informação sejam realizadas de uma forma confiável, responsável e efetiva	PC01

Promover o comportamento responsável em segurança da informação	Estimular uma cultura positiva de segurança da informação para exercer uma influência positiva no comportamento dos usuários finais, reduzir a probabilidade de ocorrência de incidentes de segurança e limitar o seu potencial impacto nos negócios	PC02

Fonte: Elaborado pelo autor (2015)

3 ANÁLISE DAS PSCI DOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA

Antes de realizarmos a análise das POSIC, é importante ressaltar que foi realizado análise por amostragem de apenas 10 (dez) órgãos da administração pública federal direta, onde escolhemos órgãos de diferentes áreas de atuação (estratégico, essencial e especial), com intuito de realizarmos uma análise comparativa destas POSIC com as melhores práticas levantadas, dentre os quarenta órgãos atualmente existentes na administração pública federal direta (Presidência da República e 39 Ministérios).

Os dez órgãos - da administração pública federal direta - que faremos a análise dos requisitos necessários das POSIC, conforme as melhores práticas, são:

a) Ministério da Defesa;
b) Ministério da Justiça;
c) Ministério da Saúde;
d) Ministério da Ciência e Tecnologia e Inovação;
e) Ministério do Planejamento, Orçamento e Gestão;
f) Ministério da Cultura;
g) Ministério do Turismo;
h) Ministério do Trabalho e Emprego;
i) Ministério da Educação;

j) Ministério da Agricultura.

3.1 Análise da POSIC dos Órgãos

3.1.1 POSIC do Ministério da Defesa

O Ministério da Defesa é o órgão do Governo Federal incumbido de exercer a direção superior das Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, articulando as ações que envolvam estas instituições, individualmente ou em conjunto. Por meio da Portaria nº 1530, publicada em 14 de maio de 2013, do Ministério da Defesa, foi instituída a Política de Segurança da Informação e Comunicação deste órgão. Nela verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²] estão previstos neste documento.

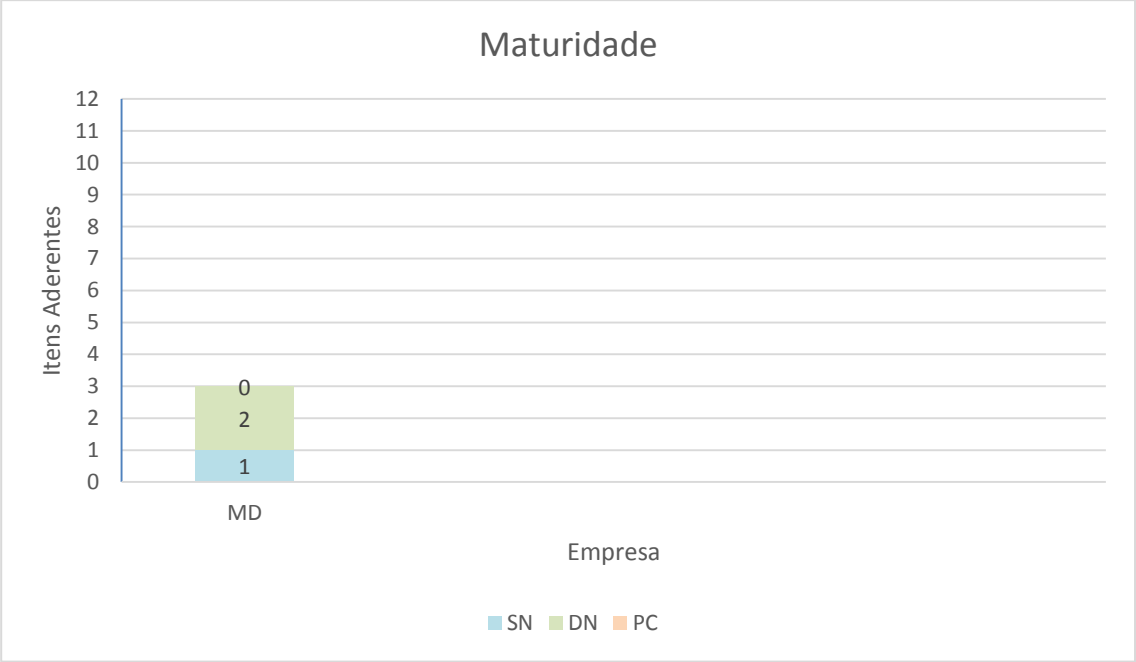
Quadro 4 – Análise da POSIC do Ministério da Defesa

CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Não	N/A
SN02	Não	N/A
SN03	Sim	1.2, 4.2, 4.3, 5.3.4, 5.3.7, 5.3.8, 5.7.2, 5.10.1, 5.13.1, 5.14.1, 5.15.1, 6, 7.1.7, 7.2.3 e 7.6.10
SN04	Não	N/A
SN05	Não	N/A
SN06	Não	N/A
DN01	Sim	5.5
DN02	Sim	5.3, 5.14
DN03	Não	N/A
DN04	Não	N/A
PC01	Não	N/A
PC02	Não	N/A

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério da Defesa podem ser vistos no quadro 4, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 1, conforme consolidado na figura 16.

Figura 16 – Maturidade do Ministério da Defesa



Fonte: Elaborado pelo autor (2015)

3.1.2 POSIC do Ministério da Justiça

O Ministério da Justiça (MJ) é um órgão autônomo da administração pública federal brasileira que trata das matérias relacionadas com a ordem jurídica, cidadania e garantias pessoais. Por meio da Portaria nº 3530, publicada em 03 de dezembro de 2013, do Ministério da Justiça que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²], estão previstos neste documento.

Quadro 5 – Análise da POSIC do Ministério da Justiça

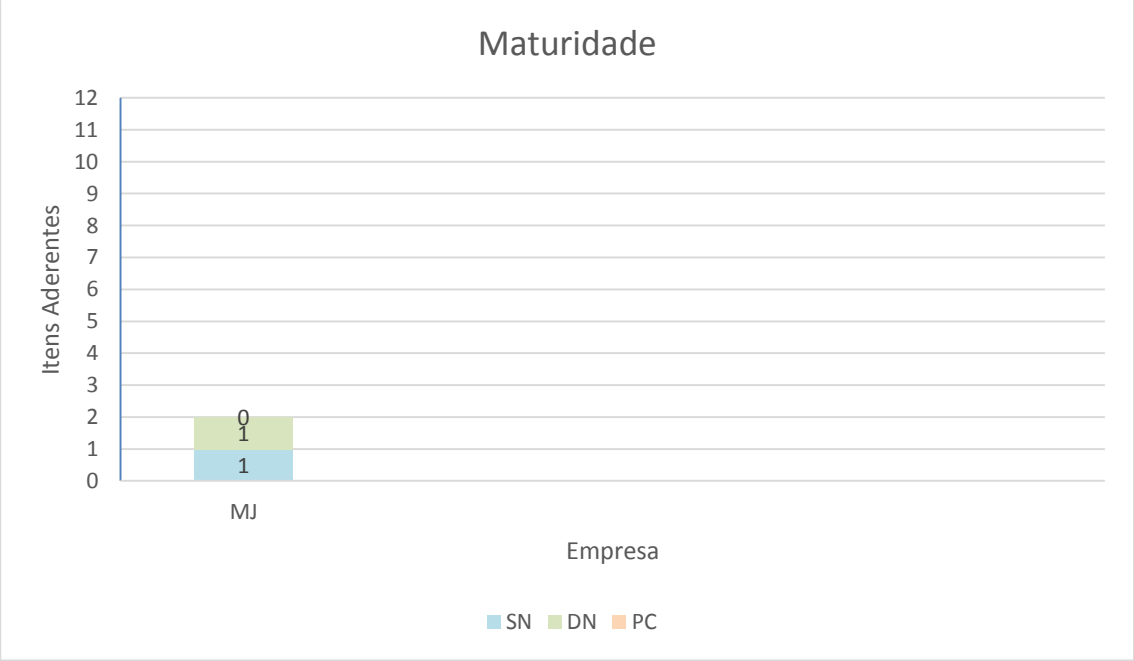
CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Não	N/A
SN02	Não	N/A
SN03	Não	N/A
SN04	Não	N/A
SN05	Sim	Art. 9º
SN06	Não	N/A
DN01	Não	N/A
DN02	Sim	Art. 4º § I
DN03	Não	N/A
DN04	Não	N/A

PC01	Não	N/A
PC02	Não	N/A

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério da Justiça podem ser vistos no quadro 5, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 1, conforme consolidado na figura 17.

Figura 17 – Maturidade do Ministério da Justiça



Fonte: Elaborado pelo autor (2015)

3.1.3 POSIC do Ministério da Saúde

O Ministério da Saúde (MS), é o setor responsável pela administração e manutenção da saúde pública do país. Por meio da Portaria nº 3207, publicada em 20 de

outubro de 2010, do Ministério da Justiça que instituiu a POSIC deste órgão, verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²], estão previstos neste documento.

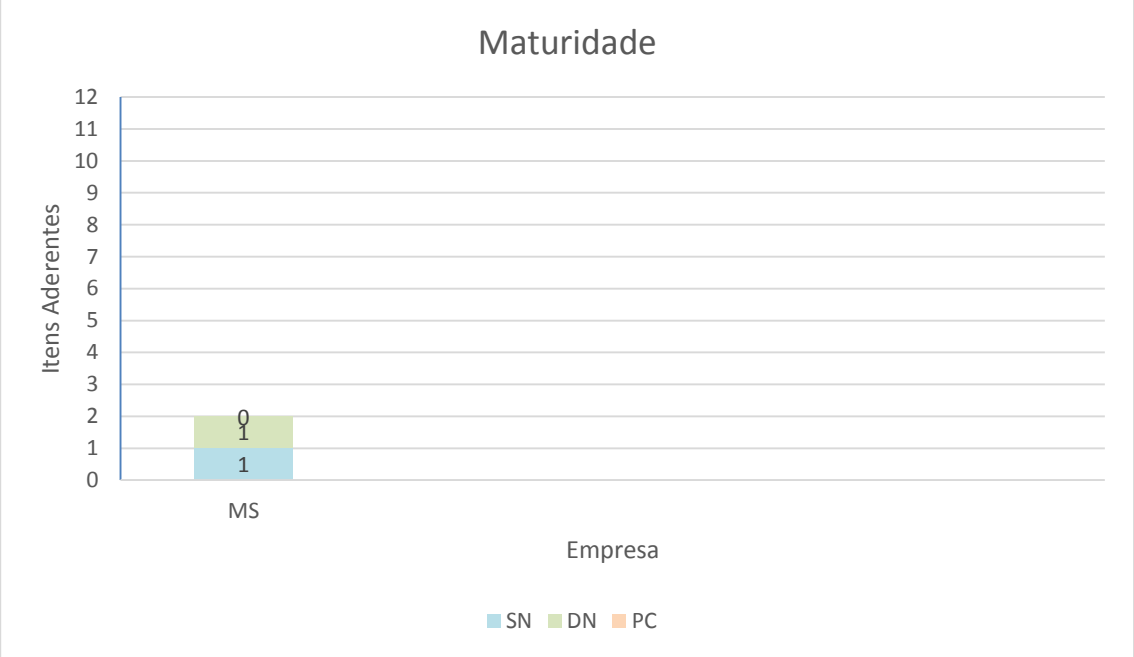
Quadro 6 – Análise da POSIC do Ministério da Saúde

CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Não	N/A
SN02	Não	N/A
SN03	Sim	Introdução, Art. 18.
SN04	Não	N/A
SN05	Não	N/A
SN06	Não	N/A
DN01	Não	N/A
DN02	Sim	Art. 4º
DN03	Não	N/A
DN04	Não	N/A
PC01	Não	N/A
PC02	Não	N/A

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério da Saúde podem ser vistos no quadro 6, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 1, conforme consolidado na figura 18.

Figura 18 – Maturidade do Ministério da Saúde



Fonte: Elaborado pelo autor (2015)

3.1.4 POSIC do Ministério da Ciência, Tecnologia e Inovação

O Ministério da Ciência, Tecnologia e Inovação (MCTI) pertence à administração direta do governo federal do Brasil, responsável pela formulação e implementação da Política Nacional de Ciência e Tecnologia, e tem suas ações pautadas nas disposições do Capítulo IV da Constituição Federal de 1988. Por meio da Portaria nº 853, publicada em 05 de setembro de 2013, do Ministério da Ciência, Tecnologia e Inovação que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²], estão previstos neste documento.

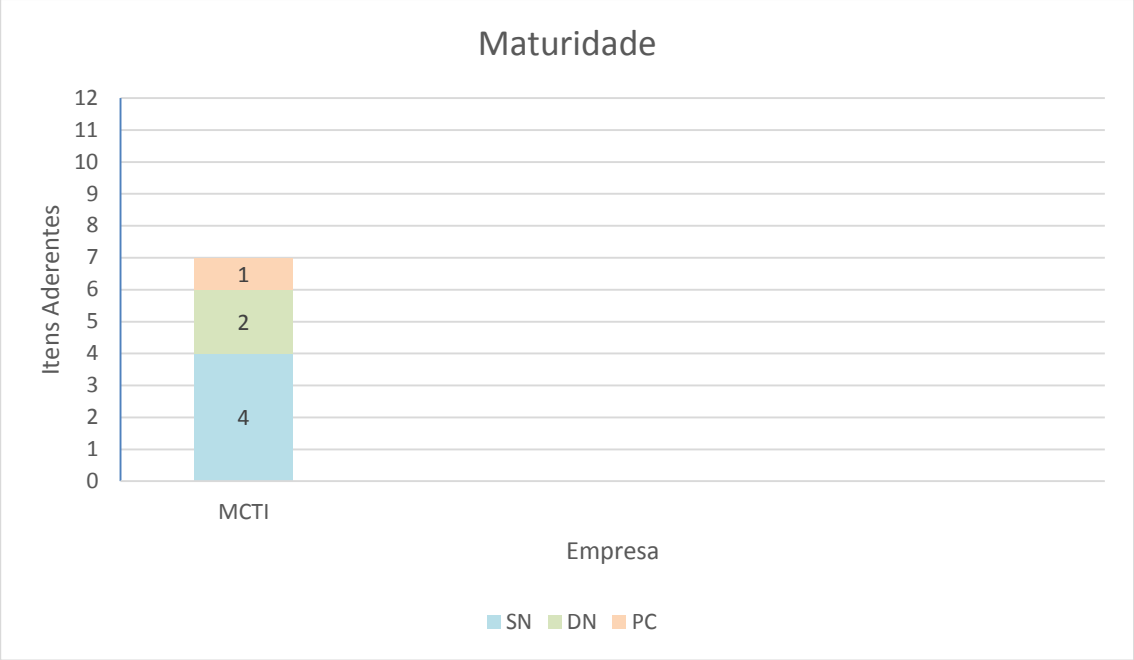
Quadro 7 – Análise da POSIC do Ministério da Ciência, Tecnologia e Inovação

CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Sim	Art. 11, Art. 12
SN02	Sim	Art. 21 e Art. 22
SN03	Sim	CAPÍTULO III
SN04	Não	N/A
SN05	Não	N/A
SN06	Sim	Art. 14 e Art. 74
DN01	Sim	Art. 48
DN02	Sim	Art. 10 e Art. 11, Art. 17, Art. 23, Art. 52
DN03	Não	N/A
DN04	Não	N/A
PC01	Não	N/A
PC02	Sim	Art. 46, Art. 47 e Art. 72 § I

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério da Ciência, Tecnologia e Inovação podem ser vistos no quadro 7, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 3, conforme consolidado na figura 19.

Figura 19 – Maturidade do Ministério da Ciência, Tecnologia e Inovação



Fonte: Elaborado pelo autor (2015)

3.1.5 POSIC do Ministério do Planejamento, Orçamento e Gestão

O Ministério do Planejamento, Orçamento e Gestão (MPOG) é um Ministério do Poder Executivo do Brasil. Sua função é planejar a administração governamental, planejar custos, analisar a viabilidade de projetos, controlar orçamentos, liberar fundos para estados e projetos do governo. Por meio da Portaria nº 142, publicada em 18 de novembro de 2011, do Ministério do Planejamento, Orçamento e Gestão/MPOG que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²], estão previstos neste documento.

Quadro 8 – Análise da POSIC do Ministério do Planejamento, Orçamento e Gestão

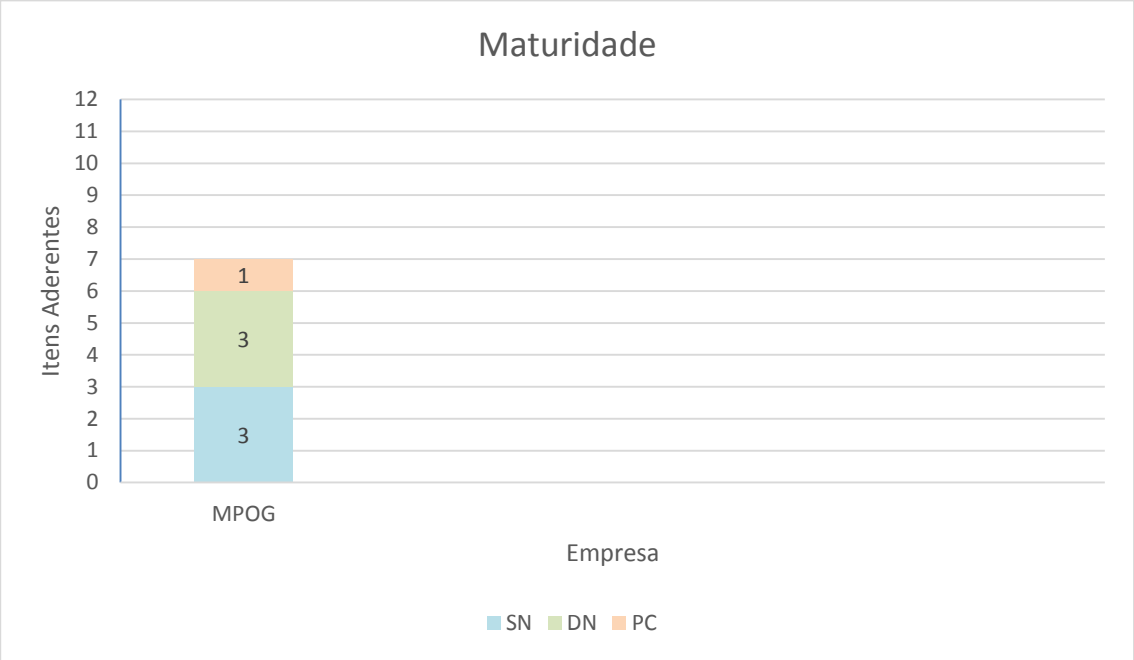
CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Sim	Art. 5º e Art. 6º
SN02	Não	N/A
SN03	Sim	Capítulo IX e Art. 56

SN04	Não	N/A
SN05	Não	N/A
SN06	Sim	Art. 12 § VI, Art. 30 e Art. 59 § V
DN01	Sim	Art. 29, Art. 30, Art. 55
DN02	Sim	Art. 2º, Art. 18, Art. 47, Seção VI
DN03	Não	N/A
DN04	Sim	Art. 48 e Art. 49
PC01	Não	N/A
PC02	Sim	Art. 58 § I e Art. 59 § VI

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério do Planejamento, Orçamento e Gestão podem ser vistos no quadro 8, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 3, conforme consolidado na figura 20.

Figura 20 – Maturidade do Ministério do Planejamento, Orçamento e Gestão



Fonte: Elaborado pelo autor (2015)

3.1.6 POSIC do Ministério da Cultura

O Ministério da Cultura (MinC) é responsável pelas letras, artes, folclore e outras formas de expressão da cultura nacional. Por meio da Portaria nº 119, publicada em 05 de dezembro de 2011, do MinC que instituiu a POSIC deste órgão, verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²], estão previstos neste documento.

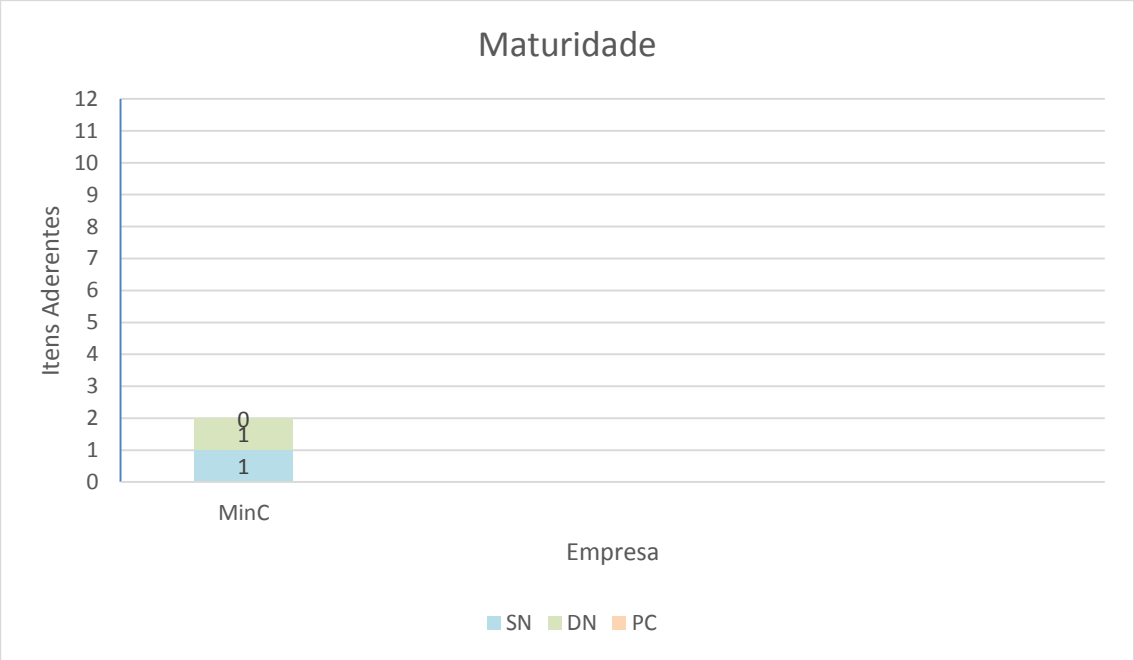
Quadro 9 – Análise da POSIC do Ministério da Cultura

CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Não	N/A
SN02	Não	N/A
SN03	Não	N/A
SN04	Não	N/A
SN05	Não	N/A
SN06	Sim	Art. 9 § III
DN01	Não	N/A
DN02	Sim	Art. 5 § V e Art. 15 § III
DN03	Não	N/A
DN04	Não	N/A
PC01	Não	N/A
PC02	Não	N/A

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério da Cultura podem ser vistos no quadro 9, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 1, conforme consolidado na figura 21.

Figura 21 – Maturidade do Ministério da Cultura



Fonte: Elaborado pelo autor (2015)

3.1.7 POSIC do Ministério do Turismo

O Ministério do Turismo (MTur) objetiva desenvolver o turismo como atividade econômica autossustentável em geração de empregos e divisas, proporcionando inclusão social. Por meio da Portaria nº 108, publicada em 22 de maio de 2013, do Ministério do Turismo que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²], estão previstos neste documento.

Quadro 10 – Análise da POSIC do Ministério do Turismo

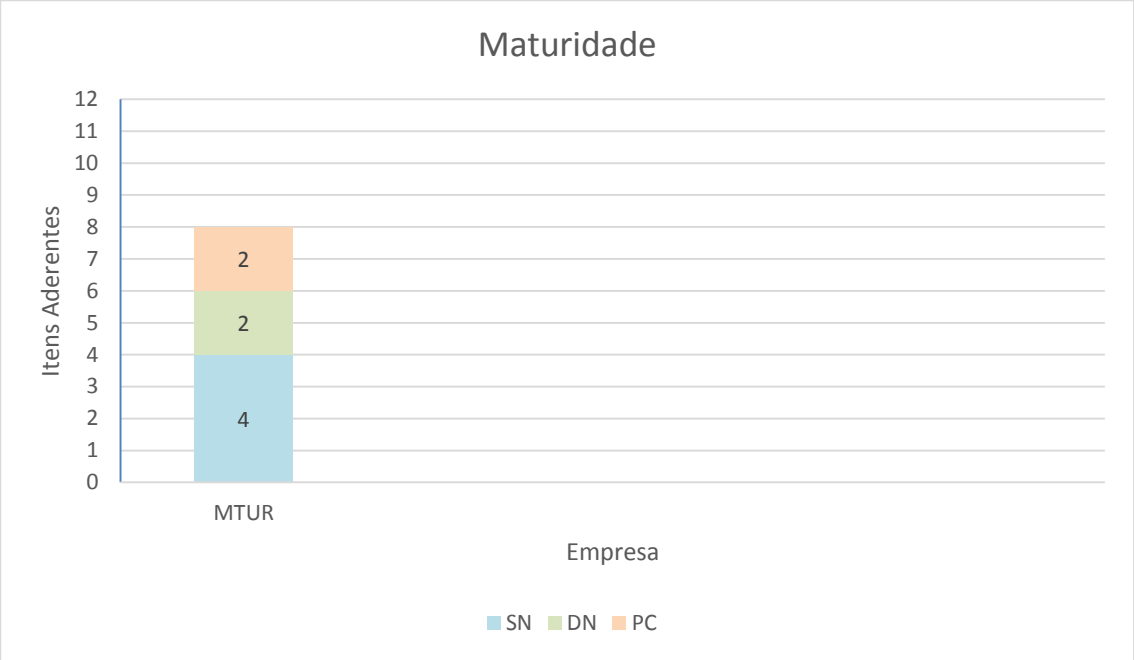
CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Sim	Art. 9 Item II, Art. 11, Art. 65
SN02	Sim	Art. 8 Item I

SN03	Sim	Art. 7 Item II e VIII, Art. 56, Art. 62, Art. 63 e Art. 64
SN04	Não	N/A
SN05	Não	N/A
SN06	Sim	Art. 9 Item VI, Art. 72
DN01	Sim	Art. 25, Art. 26 e Art. 29
DN02	Sim	Art. 24, Art. 36, Art. 54, Art. 55
DN03	Não	N/A
DN04	Não	N/A
PC01	Sim	Art. 7 Item II, V
PC02	Sim	Art. 9 Item IV, Art. 18, Art. 70 Item I

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério do Turismo podem ser vistos no quadro 10, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 4, conforme consolidado na figura 22.

Figura 22 – Maturidade do Ministério do Turismo



Fonte: Elaborado pelo autor (2015)

3.1.8 POSIC do Ministério do Trabalho e Emprego

Compete ao Ministério do Trabalho e Emprego (MTE) criar diretrizes para a geração de emprego e renda, fornecer apoio ao trabalhador, modernizar as relações do trabalho, realizar a fiscalização do trabalho, entre outras. Por meio da Portaria nº 1047, publicada

em 16 de julho de 2013, do Ministério do Trabalho e Emprego que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²], estão previstos neste documento.

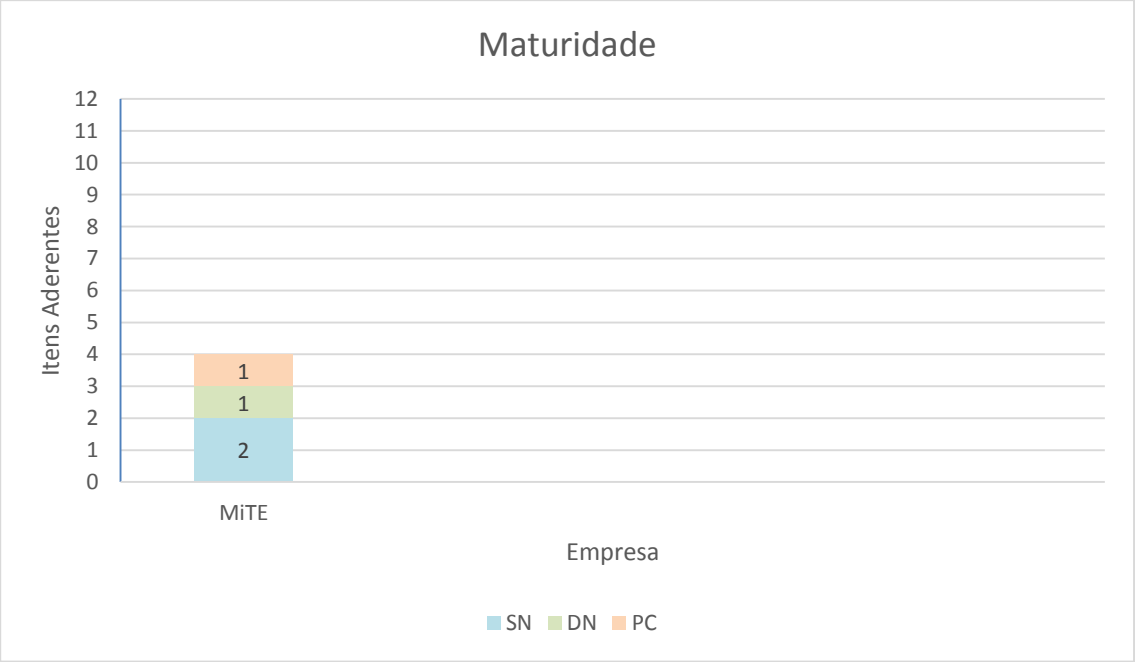
Quadro 11 – Análise da POSIC do Ministério do Trabalho e Emprego

CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Sim	Art. 8, Art. 9
SN02	Não	N/A
SN03	Sim	Art. 22, Art. 23, Art. 30, Art. 31
SN04	Não	N/A
SN05	Não	N/A
SN06	Não	N/A
DN01	Sim	Art. 15
DN02	Não	N/A
DN03	Não	N/A
DN04	Não	N/A
PC01	Não	N/A
PC02	Sim	Art. 13

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério do Trabalho e Emprego podem ser vistos no quadro 11, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 2, conforme consolidado na figura 23.

Figura 23 – Maturidade do Ministério do Trabalho e Emprego



Fonte: Elaborado pelo autor (2015)

3.1.9 POSIC do Ministério da Educação

O Ministério da Educação (MEC) é um órgão do governo federal do Brasil fundado no decreto n.º 19.402, em 14 de novembro de 1930, e tem, entre outras, competências como: política nacional de educação; educação infantil; educação em geral, compreendendo ensino fundamental, ensino médio e ensino superior. Por meio da Portaria nº 1054, publicada em 02 de agosto de 2011, do Ministério da Educação que instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²], estão previstos neste documento.

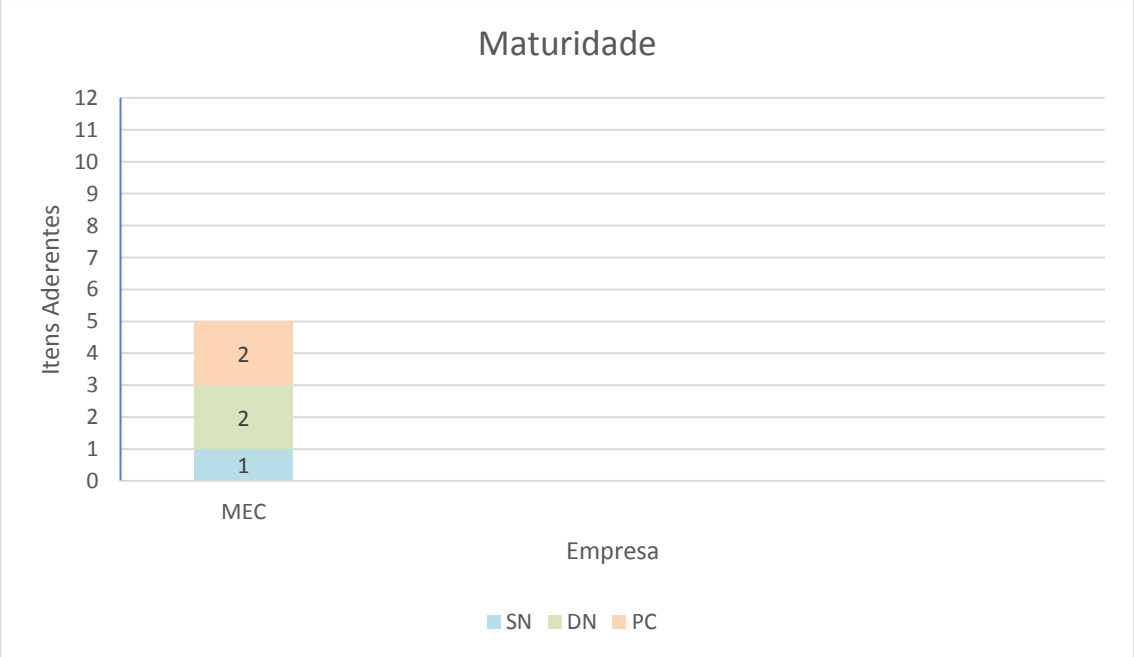
Quadro 12 – Análise da POSIC do Ministério da Educação

CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Não	N/A
SN02	Não	N/A
SN03	Sim	Art. 6, Art. 31
SN04	Não	N/A
SN05	Não	N/A
SN06	Não	N/A
DN01	Sim	Art. 19
DN02	Sim	Art. 8, Art. 10, Art. 11, Art. 29
DN03	Não	N/A
DN04	Não	N/A
PC01	Sim	Art. 7 Item II
PC02	Sim	Art. 18

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério da Educação podem ser vistos no quadro 12, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 2, conforme consolidado na figura 24.

Figura 24 – Maturidade do Ministério da Educação



Fonte: Elaborado pelo autor (2015)

3.1.10 POSIC do Ministério da Agricultura

O Ministério da Agricultura, Pecuária e Abastecimento (MAPA) é um ministério do Poder Executivo do Brasil cuja competência é formular e implementar as políticas para o desenvolvimento do agronegócio, integrando os aspectos de mercado, tecnológicos, organizacionais e ambientais, para o atendimento dos consumidores do país e do exterior, promovendo segurança alimentar, geração de renda e emprego, redução das desigualdades e inclusão social. Por meio da Portaria nº 795, publicada em 05 de setembro de 2012, do Ministério da Agricultura instituiu a Política de Segurança da Informação e Comunicação deste órgão, verificou-se quais princípios, segundo o ISACA, ISF e [(ISC)²], estão previstos neste documento.

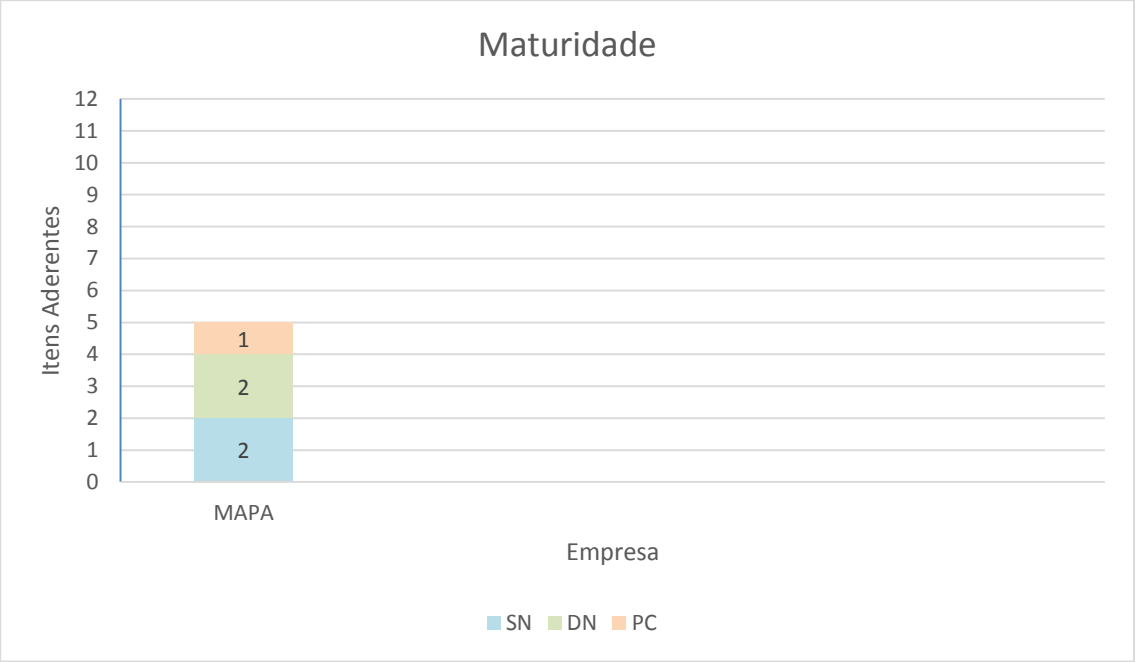
Quadro 13 – Análise da POSIC do Ministério da Agricultura

CÓDIGO	ADERENTE AOS PRINCÍPIOS	ITEM
SN01	Não	N/A
SN02	Não	N/A
SN03	Sim	Anexo I, Item 7
SN04	Não	N/A
SN05	Não	N/A
SN06	Sim	Item 5.1, 6.3
DN01	Sim	Item 5.12
DN02	Sim	Item 5.4
DN03	Não	N/A
DN04	Não	N/A
PC01	Não	N/A
PC02	Sim	Item 6.4 a

Fonte: Elaborado pelo autor (2015)

Os resultados da análise dos dados do Ministério da Agricultura podem ser vistos no quadro 13, de acordo com o grupo dos princípios analisados. O nível de maturidade obtido pela empresa foi 2, conforme consolidado na figura 25.

Figura 25 – Maturidade do Ministério da Agricultura



Fonte: Elaborado pelo autor (2015)

3.2 Requisitos consolidados das POSIC

Quadro 14 – Requisitos consolidados das POSIC

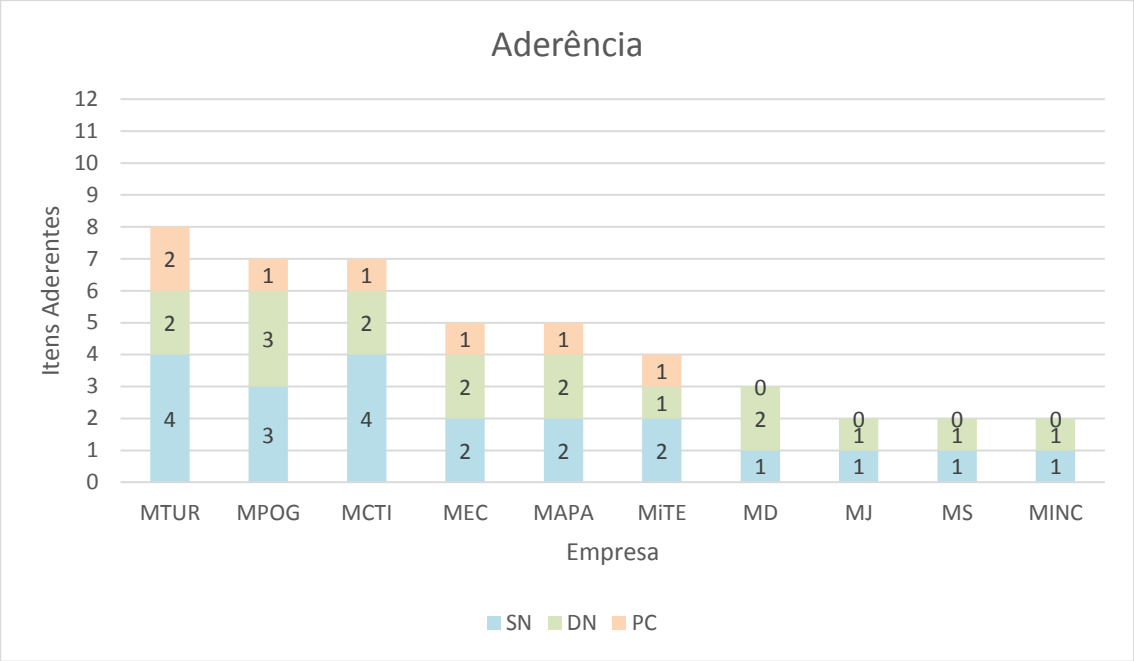
Princípios ISACA ISF [(ISC)²]	Ministério da Defesa	Ministério da Justiça	Ministério da Saúde	Ministério da Ciência e Tecnologia	Ministério do Planejamento	Ministério da Cultura	Ministério do Turismo	Ministério do Trabalho e Emprego	Ministério da Educação	Ministério da Agricultura
SN01				x	x		x	x		
SN02				x			x			
SN03	x		x	x	x		x	x	x	x
SN04										
SN05		x								
SN06				x	x	x	x			x
DN01	x			x	x		x	x	x	x
DN02	x	x	x	x	x	x	x		x	x
DN03										
DN04					x					
PC01							x		x	
PC02				x	x		x	x	x	x

Fonte: Elaborado pelo autor (2015)

Com as POSIC analisadas no item anterior, foi consolidado, por meio do quadro 14, quais princípios, segundo o ISACA, ISF e [(ISC)²], são atendidos ou não por cada Ministério analisado.

3.3 Análise das Informações Consolidadas

Figura 26 – Aderência dos princípios de segurança da informação

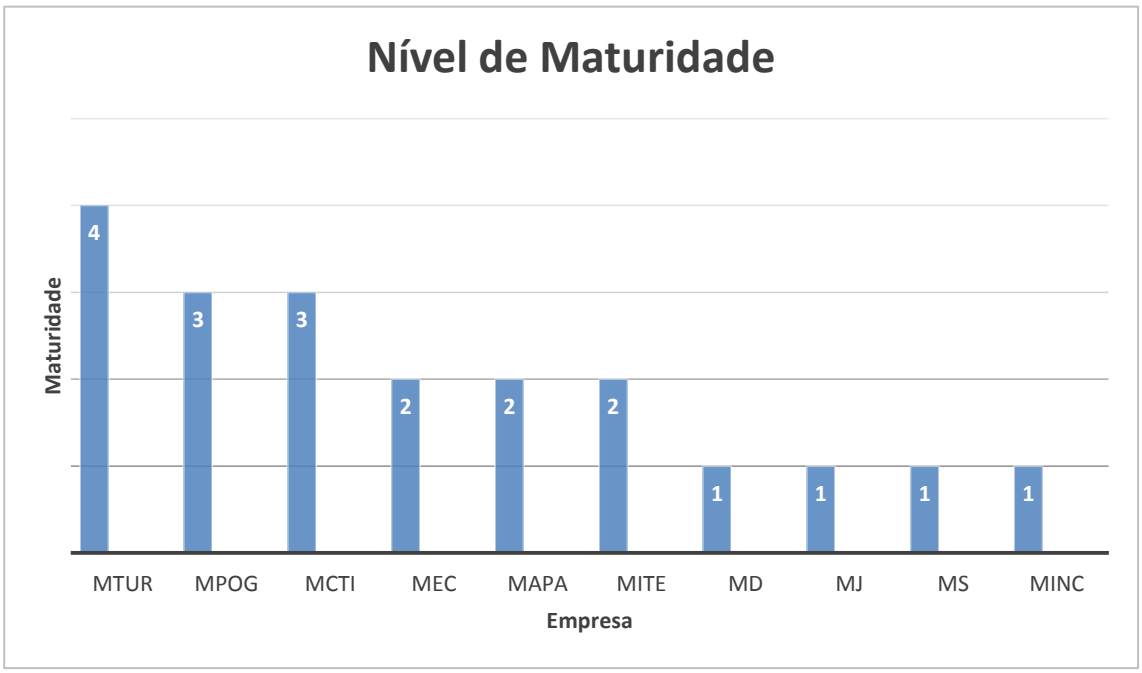


Fonte: Elaborado pelo autor (2015)

3.3.1 Análise

Ao analisar os resultados obtidos, foi possível observar uma grande variação na maturidade dos ministérios, como pode ser visto na figura 26. Este resultado surpreende, pois são fiscalizados pelo mesmo órgão competente, o Tribunal de Contas da União, e são sujeitos aos mesmos regulamentos e legislações, com isso, era esperado um maior nivelamento.

Figura 27 – Nível de maturidade dos ministérios



Fonte: Elaborado pelo autor (2015)

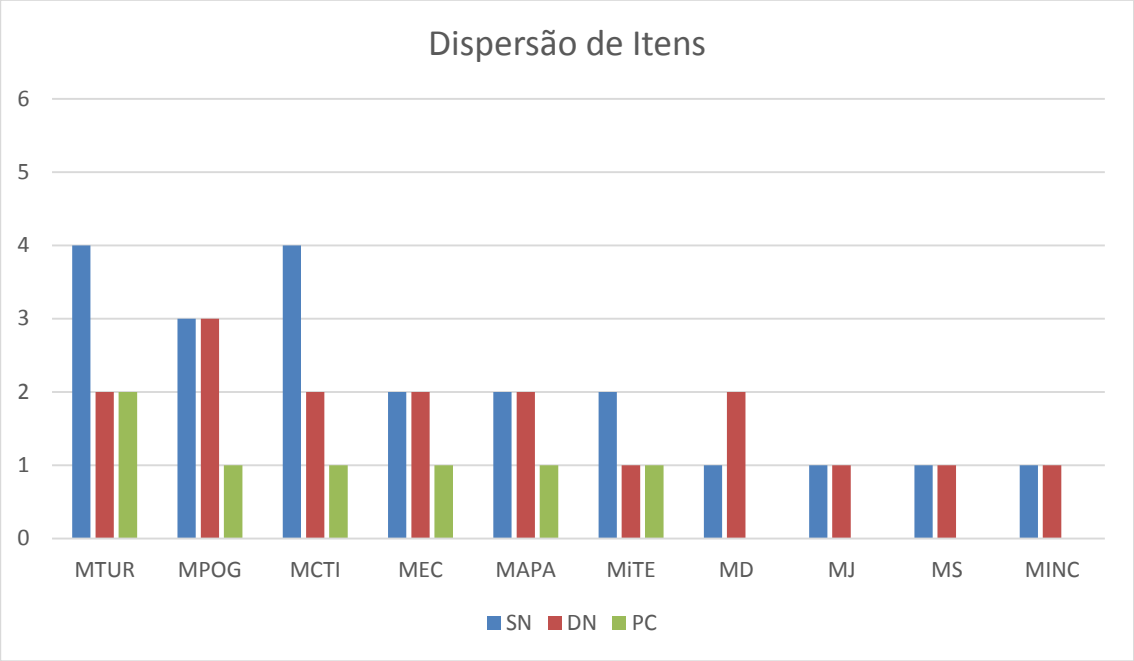
Foi possível observar também, que apesar do ramo, a Política de Segurança do Ministério do Turismo, apresentou uma maior aderência aos princípios propostos.

Enquanto Ministérios do setor estratégico, como Planejamento e Ciência e Tecnologia, onde esperava-se uma maior abordagem dos princípios, apenas sete itens, dos doze, foram atendidos. Também do setor estratégico, os Ministérios da Defesa e Justiça apresentou uma baixa maturidade e totalmente desnivelados com relação aos demais do setor. Mais focados em segurança como um fator isolado, a abordagem das POSIC do MTUR e MCTI se mostraram mais preocupados com o negócio. Isto pode ser observado na quantidade de itens do aspecto “Suportar o Negócio” que foram atendidos.

Em contrapartida, ao analisar os dados do grupo “Defender o Negócio” e “Promover o Comportamento”, podemos observar um nivelamento por baixo entre os órgãos.

Podemos observar uma comparação da dispersão dos itens atendidos na figura 28.

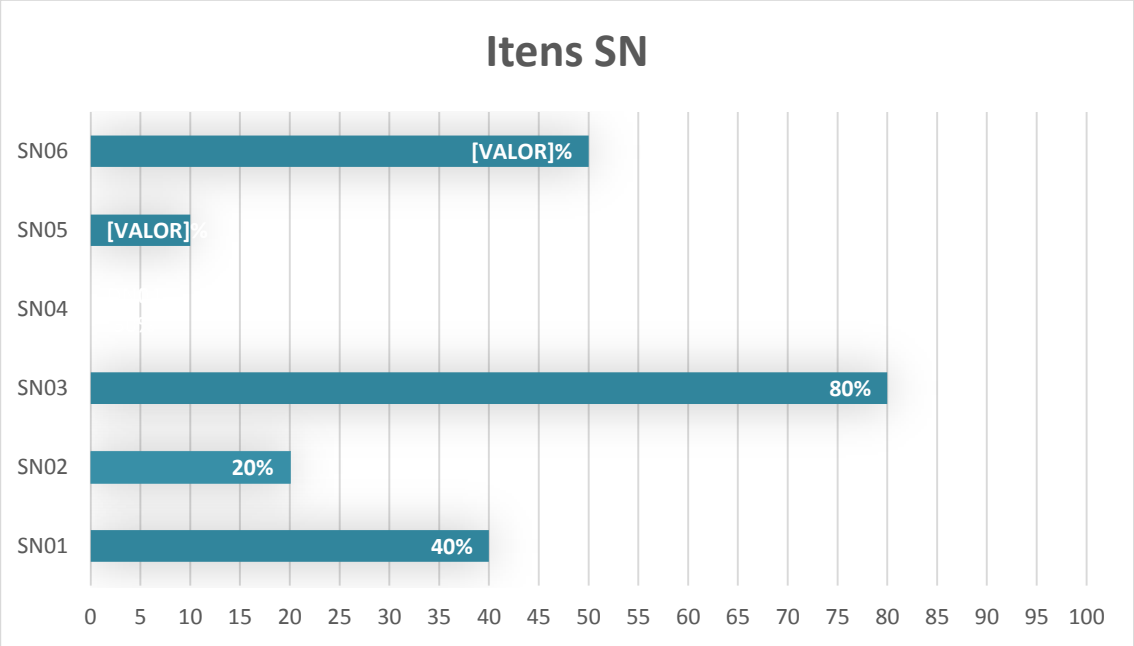
Figura 28 – Dispersão dos itens



Fonte: Elaborado pelo autor (2015)

Notamos, dentro do grupo “Suportar o Negócio”, que o princípio “Cumprir os requisitos legais e regulatórios pertinentes para garantir que obrigações estatutárias sejam cumpridos, as expectativas das partes interessadas sejam gerenciadas e penalidades civis ou criminais sejam evitadas”, foi o item mais atendido, com 8(oito) órgãos aderentes, seguidos pelos princípios “Promover a melhoria contínua em segurança da informação para reduzir custos, melhorar a eficiência e efetividade, e promover uma cultura de melhoria contínua da segurança da informação” e “Concentrar-se no negócio para garantir que a segurança da informação esteja integrada nas atividades essenciais de negócio”, como podemos verificar na figura 29.

Figura 29 – Itens aderentes do grupo Suportar o Negócio

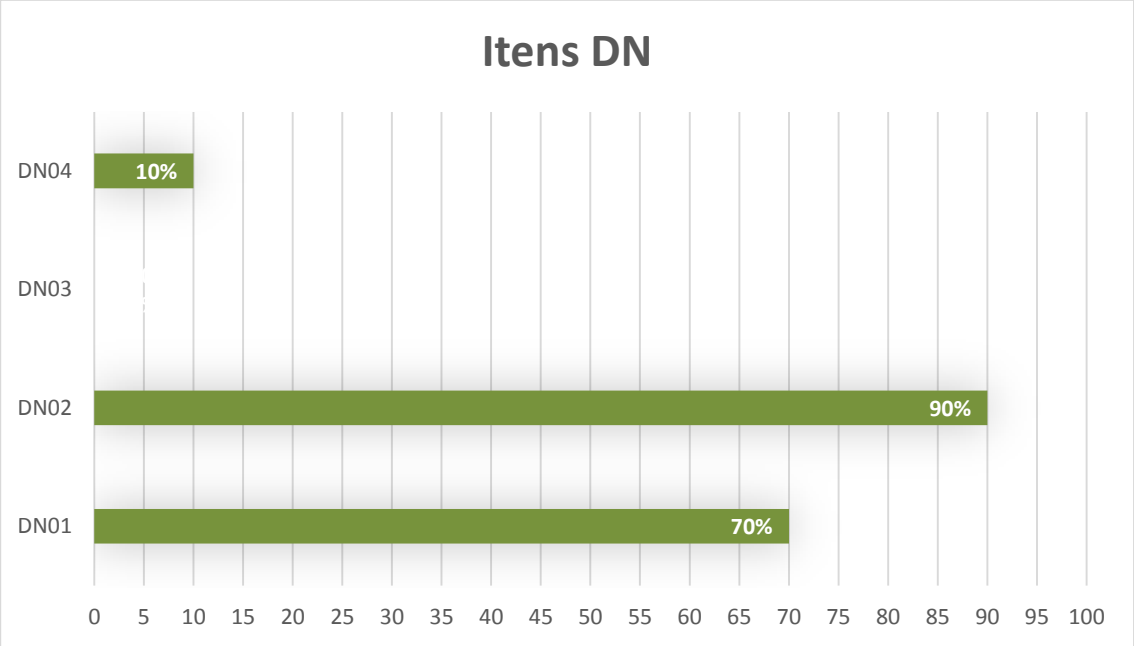


Fonte: Elaborado pelo autor (2015)

Isso mostra que a maior parte dos órgãos têm preocupação com aderência a regulamentos e legislações, pois o não cumprimento dos mesmos pode ser configurado como uma infração, sujeito às penalidades previstas em leis e sanções administrativas. Nenhum órgão preocupou-se em atender o princípio “Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação para apoio aos requisitos de negócio e gerenciar o risco da informação”, isso significa que se preocupam em defender a informação, mas não em manter uma forma de medir a situação atual para gerenciar a segurança.

Ao analisar o grupo “Defender o Negócio”, temos o princípio “Proteger informações confidenciais para impedir a divulgação a pessoas não autorizadas” coberto por quase todas as políticas, seguido pelo princípio “Adotar uma abordagem baseada em risco para garantir que o risco é tratado de uma maneira consistente e efetiva” que é coberto por 70% das políticas analisadas, como pode ser visto na figura 30.

Figura 30 – Itens aderentes do grupo Defender o Negócio

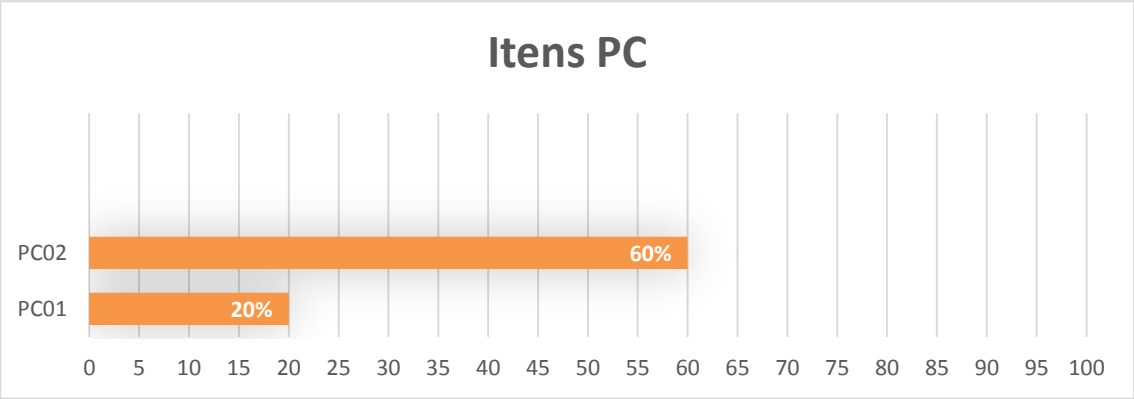


Fonte: Elaborado pelo autor (2015)

Podemos inferir que o controle do acesso às informações é uma preocupação em comum a grande maioria dos Ministérios e que a preocupação com o gerenciamento de riscos é plausível, uma vez que em 7 órgãos o item do grupo de “Defender o Negócio” mais coberto foi justamente o de gerenciamento de riscos.

Dentro do Grupo “Promover o Comportamento”, o princípio “Estimular uma cultura positiva de segurança da informação para exercer uma influência positiva no comportamento dos usuários finais, reduzir a probabilidade de ocorrência de incidentes de segurança e limitar o seu potencial impacto nos negócios” foi abordado de alguma forma por 60% das empresas da administração pública, demonstrando uma preocupação em educar seus usuários ao manusear as informações do órgão. Por se tratar de uma grande quantidade de informações sigilosas e de extrema importância, esse item decepcionou, pois acreditava-se uma maior aderência por parte das empresas. O outro princípio, “Agir de forma ética e profissional para garantir que as atividades relacionadas à segurança da informação sejam realizadas de uma forma confiável, responsável e efetiva” foi infimamente abordado, conforme figura 31.

Figura 31 – Itens aderentes do grupo Promover o Comportamento



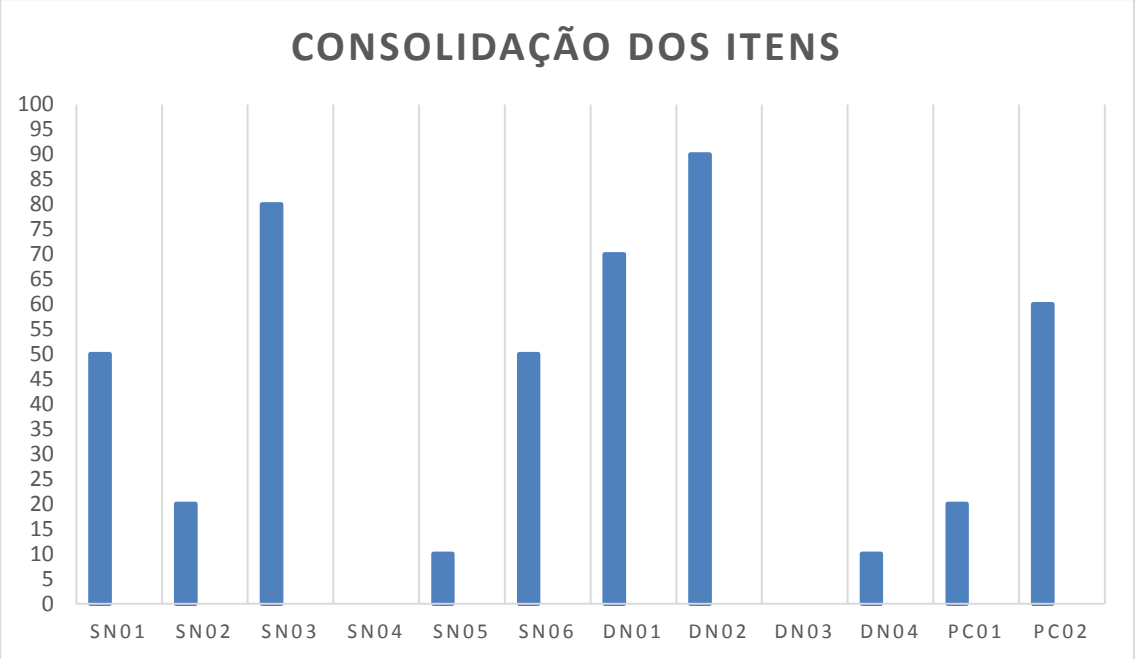
Fonte: Elaborado pelo autor (2015)

Órgãos como Ministério da Defesa, Justiça, Saúde e Cultura não possuíam itens em sua política que cubram os princípios do grupo “Promover o Comportamento”. Apesar da política ser baseada na ISO 27001, políticas de treinamento e de conscientização dos funcionários não foi inclusa no documento.

Ao analisar os itens com menor cobertura dentro da políticas analisadas, os princípios “Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação para apoio aos requisitos de negócio e gerenciar o risco da informação" e "Concentrar-se em aplicações críticas de negócios para priorizar recursos escassos de segurança da informação, protegendo as aplicações de negócio nas quais um incidente de segurança teria o maior impacto nos negócios”, dos grupos “Suportar o Negócio” e “Defender o Negócio” respectivamente, não foram previstos por nenhuma POSIC das empresas analisadas, o que demostra, como citado anteriormente, que não existiu uma preocupação nas métricas atuais de segurança da informação para apoiar o negócio e protege-lo através dos serviços críticos mitigando o risco de um incidente grave de segurança.

Podemos observar na figura 32, como ficou o percentual de empresas aderentes a cada item de forma consolidada. O que nos dá uma visão dos itens com maior e menor cobertura.

Figura 32 – Consolidação dos itens



Fonte: Elaborado pelo autor (2015)

CONCLUSÃO

No estudo realizado, conclui-se, por meio de análise das políticas de segurança da informação e comunicação, documentos, portarias, leis e decretos, que as empresas da administração pública federal preocupa-se em construir suas POSIC baseadas somente nas melhores práticas da ISO 27002 visando apenas atender as normas exigidas pelos órgãos fiscalizadores, não preocupando em, de fato, suportar e defender o negócio promovendo um comportamentos de segurança responsável.

No estudo, foi verificado que o governo federal está direcionando seus esforços para que a implementação da segurança da informação seja realizada em compliance com as leis e melhores práticas, ainda que apresentem uma maturidade diversificada, em sua maioria abaixo do esperado no início da pesquisa.

Existe a necessidade de uma melhor orientação para que haja uma maior homogeneidade e maturidade nessas empresas, afim de utilizar as políticas de segurança da informação como um viabilizador, agregando valor ao negócio, não apenas um mero documento.

Inferiu-se também que, nenhum ministério atendeu em sua totalidade aos 12 princípios propostos pelo consórcio. Avaliando individualmente cada grupo, a preocupação com o nível estratégico é minimizada ao observamos que princípios baseados na entrega de valor e melhoria continua não são prioridade, porém princípios baseados em controle de acesso e gerenciamento de riscos são focos comuns na maioria das empresas.

A importância da adoção de princípios orientadores para os profissionais de segurança da informação está sobretudo relacionada com a necessidade de harmonizar comportamentos para que seja possível o desenvolvimento de uma verdadeira cultura de valorização da informação como um ativo crítico dos ministérios e consequentemente da importância em garantir sua confidencialidade, integridade e disponibilidade.

Como qualquer outra lei escrita por homens terá as suas vulnerabilidades e estará exposta a ameaças. No entanto, qualquer organização deverá começar por definir e comunicar as suas políticas para que todos os envolvidos possam ter conhecimentos das regras corporativas de segurança da informação.

REFERÊNCIAS

ABNT. Tecnologia da informação - Técnicas de segurança - **Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2013**. 2a. ed. Rio de Janeiro, 2013.

ABNT. Tecnologia da informação - Técnicas de segurança - **Sistemas de gestão de segurança da informação - Requisitos: ABNT NBR ISO/IEC 27001:2006**. 1a. ed. Rio de Janeiro, 2006.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações** – São Paulo: Atlas, 2005.

CAMPOS, André L. N. **Sistema de segurança da informação: controlando os riscos**. Florianópolis: Visual Books, 2006.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações –** São Paulo: Editora SENAC São Paulo, 1999.

CASTRO, Mauro. **Política de Tecnologia da Informação no Brasil (Um guia para o século XXI)**. 1.ed.: Politec, 2002.

CERNEV, Adrian Kemmer; LEITE, Jaci Corrêa. **Segurança na Internet: a percepção dos usuários como fator de restrição ao comércio eletrônico no Brasil** – ENANPAD, 2005.

Decreto nº. 3.505, de 13 de junho de 2000: Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. BRASIL. Disponível em: www.planalto.gov.br/ccivil_03/decreto/D3505.htm. Acesso em: 14 out 2015.

DE HAES, Steven; VAN GREMBERGEN, Wim; DEBRECENY, Roger S. COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. **Journal of Information Systems**, v. 27, n. 1, p. 307-324, 2013.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna LTDA., 2003.

FERREIRA, F.N.F.; ARAÚJO, M.T. **Política de Segurança da Informação – Guia Prático para Elaboração e Implementação**. Rio de Janeiro: Editora Ciência Moderna LTDA., 2006.

FONTES, Edson. **Segurança da Informação: o usuário faz a diferença**. Microsoft, São Paulo. Editora Saraiva, 2006.

Instrução Normativa GSI Nº 01, DE 13 DE JUNHO DE 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta. Disponível em: http://dsic.planalto.gov.br/documentos/nc_7_controle_acesso.pdf. Acesso em: 14 out 2015.

International Organization for Standardization and International Electrotechnical Commission, **ISO/IEC 27002: 2005, Information technology—Security techniques—Code of practice for information security controls**, 2015, www.iso27001security.com/html/27002.html . Acesso em: 08 set 2015.

ISACA, **COBIT® 5 for Information Security**, USA, 2012, http://www.isaca.org/cobit/pages/info-sec.aspx . Acesso em: 08 set 2015.

LYRA, Mauricio. **Governança da Segurança da Informação** Brasília, 2015.

LYRA, Maurício; FERRER, J. (2015), Checking the Maturity of Security Policies for Information and Communication. **ISACA Journal**, Volume 2. Disponível em:

http://www.isaca.org/Journal/archives/2015/Volume-2/Pages/checking-the-maturity-of-security-policies-for-information-and-communication.aspx Acesso em: 02 nov 2015.

LYRA, Maurício; TORMIM, K.; NISHI, Vitor (2016), Maturity Security Information Governance: Applied to the Telecom Segment in Brazil. **ISACA Journal**, Volume 1. Disponível em: http://www.isaca.org/Journal/archives/2016/Volume-1/Pages/maturity-security-information-governance.aspx. Acesso em: 15 jan 2016.

MARTINS, José Carlos Cordeiro. **Gestão de Projetos de Segurança da Informação**. Rio de Janeiro, Brasport: 2003.

MONTEIRO, Edmundo; BOAVIDA, Fernando, **Engenharia de Redes Informáticas**, 4ª ed., FCA Editora de Informática Ltda, 2000.

NAKAMURA, E., GEUS, P. **Segurança de redes em ambientes cooperativos: fundamentos, técnicas, tecnologias, estratégias**. São Paulo: Novatec, 2003.

Portaria nº 108, de 22/05/2013/Ministério do Turismo. Institui a Política de Segurança da Informação e Comunicação - POSIC, no âmbito do Ministério do Turismo. Disponível em: http://www.turismo.gov.br/turismo/legislacao/portarias/20130523.html. Acesso em: 08 set 2015.

Portaria nº 119, de 05/12/2011/MinC – Ministério da Cultura. Institui a Política de Segurança da Informação e Comunicações do Ministério da Cultura e o Sistema de Segurança da Informação e Comunicações. Disponível em: http://www2.cultura.gov.br/site/2011/12/07/portaria-n%C2%BA-1192011minc/. Acesso em: 08 set 2015.

Portaria nº 142, de 18/11/2011/SOF – Secretaria do Orçamento Federal/MPOG. Institui a Política de Segurança da Informação e Comunicação – PoSIC da Secretaria de Orçamento Federal/MPOG. Disponível em:

http://www.orcamentofederal.gov.br/orcamentos-anuais/orcamento-2011/programacao-orcamentaria-e-financeira/portaria-sof/Ptr_sof_142_de_181111.pdf/at_download/file . Acesso em: 08 set 2015.

Portaria nº 795, de 5/09/12/Ministério da Agricultura. Aprovar a atualização da Política de Segurança da Informação e Comunicações do Ministério da Agricultura, Pecuária e Abastecimento. Disponível em: http://www.agricultura.gov.br/arq_editor/file/acesso_informacao/pregao/Documentos-PREGAO-20-2013/10-Politica-Seguranca-Informacao-Comunicacoes.pdf. Acesso em: 08 set 2015.

Portaria nº 853, de 05/09/2013/MCTI - Ministério da Ciência e Tecnologia e Inovação. Institui a Política de Segurança da Informação e Comunicações do Ministério da Ciência, 67 Tecnologia e Inovação (Posic/MCTI). Disponível em: http://www.jusbrasil.com.br/diarios/58795774/dou-secao-1-06-09-2013-pg-7. Acesso em: 08 set 2015.

Portaria nº 1047 de 16/07/2013 / MTE - Ministério do Trabalho e Emprego. Institui a Política de Segurança da Informação e Comunicações – POSIC do Ministério do Trabalho e Emprego. Disponível em: http://www.diariodasleis.com.br/busca/exibelink.php?numlink=224048. Acesso em: 08 set 2015.

Portaria n° 1054, de 02/08/2011/Ministério da Educação e suas alterações na Portaria nº 996 de 06/08/2012. Aprova a Política de Segurança da Informação e Comunicações - POSIC do Ministério da Educação – MEC. Disponível em: http://www.educacao.gov.br/index.php?option=com_content&view=article&id=15451&Itemid=1078. Acesso em: 08 set 2015.

Portaria nº 1530, de 14/05/13/Ministério da Defesa. Institui a Política de Segurança da Informação e Comunicações da Administração Central do Ministério da Defesa. Disponível

em: http://www.jusbrasil.com.br/diarios/54405781/dou-secao-1-16-05-2013-pg-33. Acesso em: 08 set 2015.

Portaria nº 3.207, de 20/10/2010/Ministério da Saúde. Institui a Política de Segurança da Informação e Comunicações do Ministério da Saúde. Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2010/prt3207_20_10_2010.html. Acesso em: 08 set 2015.

Portaria nº 3.530, de 3/12/2013/Ministério da Justiça. Institui a Política de Segurança da Informação e Comunicações do Ministério da Justiça. Disponível em: http://www.jusbrasil.com.br/diarios/62532816/dou-secao-1-04-12-2013-pg-22. Acesso em: 08 set 2015.

REZENDE, Denis Alcides. ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Atlas, 2000.

SÊMOLA, M. **Gestão da Segurança da Informação – Uma visão executiva**. 3. Ed. Rio de Janeiro: Elsevier, 2003. 160p.

SENGUPTA, A.; MAZUMDAR C.; BAGCHI A. **A Formal Methodology for Detection of Vulnerabilities in an Enterprise Information System, In Conference on Risks and Security of Internet and Systems (CRiSIS)**, p. 74-80, October 2009.

Souza Neto, João. **Gestão e Governança de Segurança da Informação no ambiente de TI**. Material de curso. CEGSIC 2012-2014 - Curso de Especialização em Gestão da Segurança da Informação e Comunicações, UNB. 2012

SPANCESKI, R. Francini, (2004), **Política de segurança da informação – Desenvolvimento de um Modelo voltado para Instituições de ensino monografia de Bacharel, [em linha]**. Disponível em:

http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf Acesso em: 18 out 2015.

TADANO, K. Yumi. **Gestão Eletrônica de Documentos: Assinatura Digital e Validação Jurídica de Documentos Electrónicos**, Cuiabá MT – Brasil, 2002.